

# TASK ORDER

GST0013AJ0084  
Modification PO12

## INFRASTRUCTURE SUPPORT (ISC-3)

IN SUPPORT OF:

*Federal Deposit Insurance Corporation (FDIC)*  
Division of Information Technology (DIT)

**Issued to:**

**Computer Sciences Corporation (CSC)**  
**15000 Conference Center Drive**  
**Chantilly, VA 20151-3808**

**Issued by:**

**General Services Administration (GSA)**  
**The Federal Systems Integration and Management Center (FEDSIM)**  
**GSA FEDSIM (QF)**  
**3<sup>rd</sup> Floor, Wing 1**  
**1800 F Street NW**  
**Washington, DC 20405**

**February 19, 2015**

**FEDSIM Project Number FD00586 - 11044FDM**

## **SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS**

NOTE: The Section numbers in this Task Order (TO) correspond to the Section numbers in the Alliant Contract.

### **B.1 GENERAL**

The work shall be performed in accordance with all Sections of this TO and the contractor's Basic Contract, under which this TO is placed. An acronym listing to support this Task Order Request (TOR) is included in Section J.

### **B.5 CONTRACT ACCESS FEE**

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a Contract Access Fee (CAF). The amount of the CAF is  $\frac{3}{4}\%$  (i.e., (.0075)) of the total price/cost of contractor performance up to a maximum of \$100,000 per TO year. The CAF shall be obligated at Task Order Award (TOA). The CAF for this effort is \$100,000 per a 12 month period, totaling \$450,000 for the life of the TO.

### **B.6 ORDER TYPES**

The contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for Contract Line Item Numbers (CLINs) 0001, 1001, 2001, 3001, 4001, and 5001; on a Not-to-Exceed (NTE) Cost Reimbursable basis for CLINs 0002, 0003, 0004, 1002, 1003, 1004, 2002, 2003, 2004, 3002, 3003, 3004, 4002, 4003, 4004, 5002, 5003, and 5004; and on a NTE for the CAF for CLINs 0005, 1005, 2005, 3005, 4005, and 5005.

### **B.7 ORDER PRICING (ALL ORDER TYPES)**

Long-distance travel is defined as travel over 50 miles. Local travel will not be reimbursed. The following abbreviations are used in this price schedule:

CPAF	Cost-Plus-Award-Fee
CLIN	Contract Line Item Number
NTE	Not-to-Exceed
CR	Cost Reimbursable

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.7.1.1 BASE PERIOD (6 MONTHS):

#### LABOR CLIN

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
0001	Labor - Tasks 1 through 7	\$(b) (4)	\$(b) (4)	\$12,108,315

CLIN	Description	Total Estimated Cost
0002	Subcontract Labor - Tasks 1 through 7 to include Indirect Handling Rate (b) (4)%	\$3,013,415

#### TRAVEL AND ANCILLARY PRODUCTS AND SERVICES CLINs

CLIN	Description		Total Ceiling Price
0003	Long Distance Travel Including Indirect Handling Rate (b) (4)%	NTE	\$ 10,000
0004	Ancillary products and services Including Indirect Handling Rate (b) (4)% and CSC ODC fee (b) (4)%	NTE	\$1,000,000

#### CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
0005	Contract Access Fee	NTE	\$ 50,000

**TOTAL CEILING BASE PERIOD CLINs:**

**\$ 16,181,730**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.7.1.2 FIRST OPTION PERIOD (5 MONTHS, July 27, 2014 – December 31, 2014):

#### LABOR CLIN

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
1001	Labor - Tasks 1 through 7	\$(b) (4)	\$(b) (4)	\$14,574,831

CLIN	Description	Total Estimated Cost
1002	Subcontract Labor - Tasks 1 through 7 to include Indirect Handling Rate (b) (4)%	\$5,577,896

#### TRAVEL AND ANCILLARY PRODUCTS AND SERVICES CLINs

CLIN	Description		Total Ceiling Price
1003	Long Distance Travel Including Indirect Handling Rate (b) (4)%	NTE	\$40,000
1004	Ancillary products and services Including Indirect Handling Rate (b) (4)% and CSC ODC fee (b) (4)%	NTE	\$31,302,928

#### CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
1005	Contract Access Fee	NTE	\$ 50,000

**TOTAL OPTION PERIOD 1 CLINs:** **\$51,545,655**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.7.1.3 SECOND OPTION PERIOD (1 YEAR, January 1, 2015 – December 31, 2015):

#### LABOR CLIN

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
2001	Labor - Tasks 1 through 7	\$(b) (4)	\$(b) (4)	\$43,595,247

CLIN	Description	Total Estimated Cost
2002	Subcontract Labor - Tasks 1 through 7 to include Indirect Handling Rate (b) (4)%	\$7,500,000

#### TRAVEL AND ANCILLARY PRODUCTS AND SERVICES CLINs

CLIN	Description		Total Ceiling Price
2003	Long Distance Travel Including Indirect Handling Rate (b) (4)%	NTE	\$ 30,000
2004	Ancillary products and services Including Indirect Handling Rate (b) (4)% and CSC ODC fee (b) (4)%	NTE	\$ 12,900,000

#### CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
2005	Contract Access Fee	NTE	\$ 100,000

**TOTAL CEILING OPTION PERIOD 2 CLINs:**

**\$64,125,247**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.7.1.4 THIRD OPTION PERIOD: (1 YEAR, January 1, 2016 – December 31, 2016):

#### LABOR CLIN

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
3001	Labor - Tasks 1 through 7	(b) (4)	\$(b) (4)	\$35,594,980

CLIN	Description	Total Estimated Cost
3002	Subcontract Labor - Tasks 1 through 7 to include Indirect Handling Rate (b) (4)%	\$4,524,981

#### TRAVEL AND ANCILLARY PRODUCTS AND SERVICES CLINs

CLIN	Description		Total Ceiling Price
3003	Long Distance Travel Including Indirect Handling Rate (b) (4)%	NTE	\$ 60,000
3004	Ancillary products and services Including Indirect Handling Rate (b) (4)% and CSC ODC fee 0%	NTE	\$41,302,928

#### CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
3005	Contract Access Fee	NTE	\$ 100,000

**TOTAL CEILING OPTION PERIOD 3 CLINs:**

**\$81,582,800**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.7.1.5 FOURTH OPTION PERIOD (1 YEAR, January 1, 2017 – December 31, 2017):

#### LABOR CLIN

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
4001	Labor - Tasks 1 through 7	\$(b) (4)	\$(b) (4)	\$34,448,945

CLIN	Description	Total Estimated Cost
4002	Subcontract Labor - Tasks 1 through 7 to include Indirect Handling Rate (b) (4)%	\$4,520,330

#### TRAVEL AND ANCILLARY PRODUCTS AND SERVICES CLINs

CLIN	Description		Total Ceiling Price
4003	Long Distance Travel Including Indirect Handling Rate (b) (4)%	NTE	\$ 60,000
4004	Ancillary products and services Including Indirect Handling Rate (b) (4)% and CSC ODC fee (b) (4)%	NTE	\$ 41,302,928

#### CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
4005	Contract Access Fee	NTE	\$ 100,000

**TOTAL CEILING OPTION PERIOD 4 CLINs:**

**\$80,432,203**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.7.1.6 FIFTH OPTION PERIOD (7 MONTHS, January 1, 2018 – July 31, 2018):

#### LABOR CLIN

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
5001	Labor - Tasks 1 through 7	\$(b) (4)	\$(b) (4)	\$13,139,221

CLIN	Description	Total Estimated Cost
5002	Subcontract Labor - Tasks 1 through 7 to include Indirect Handling Rate (b) (4)%	\$5,700

#### TRAVEL AND ANCILLARY PRODUCTS AND SERVICES CLINs

CLIN	Description		Total Ceiling Price
5003	Long Distance Travel Including Indirect Handling Rate %	NTE	\$ 70,000
5004	Ancillary products and services Including Indirect Handling Rate % and CSC ODC fee (b) (4)%	NTE	\$ 58,054,392

#### CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
5005	Contract Access Fee	NTE	\$ 50,000

**TOTAL OPTION PERIOD 5 CLINs:** **\$71,319,313**

**GRAND TOTAL OF ALL CLINs:** **\$ 365,186,948**



## **SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS**

### **B.12      SECTION B TABLES**

#### **B.12.1    INDIRECT/MATERIAL HANDLING RATE**

Travel and ancillary products and services costs incurred may be burdened with the contractor's indirect/material handling rate commensurate with forward pricing rate agreements and if such indirect/material handling rate is not included in the fully burdened labor rate.

All indirect rates proposed and billed under this task order shall be commensurate with the then current Defense Contract Audit Agency (DCAA)-approved forward pricing rate agreement. Indirect rates include, but may not be limited to, indirect material handling rates, overhead rates, and general and administrative rates.

### **B.13      INCREMENTAL FUNDING**

#### **B.13.1    INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION**

Incremental funding for CLINs 0001 through 2005 is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs will be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through March 31, 2015, unless otherwise noted in Section B. The TO will be modified to add funds incrementally up to the maximum of \$365,186,948 over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

The Incremental Funding Chart is a separate Excel spreadsheet (See **Section J, Attachment AAAA - Incremental Funding Chart**).

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

### **C.1 BACKGROUND**

The Federal Deposit Insurance Corporation (FDIC) is a self-funded, non-appropriated entity of the Federal Government. The FDIC's mission is to preserve and promote public confidence in the U.S. financial systems by insuring deposits in banks and thrift institutions for up to \$250,000; by identifying, monitoring, and addressing risks to the deposit insurance funds; and by limiting the effect on the account and the financial system when a bank or thrift institution fails.

The FDIC Division of Information Technology (DIT) is the managing office for the current Infrastructure Support Contract (ISC), which was awarded in 2009, and the Government expects this TO, hereafter referred to as ISC3 to replace the current ISC task order, hereafter referred to as ISC2, after necessary transition. The ISC covers the day-to-day operation of FDIC's infrastructure facilities, hardware, software, and systems. It primarily supports operational security, client support/help desk, data center operations, asset management, and systems engineering service areas. The ISC3 TO will provide the support activities that facilitate FDIC's delivery of software applications by managing the underlying infrastructure, supporting release management, and providing operations and maintenance of the development, quality assurance, testing, production, and disaster recovery environments. In addition to providing information technology (IT) administration, management, and provisioning services for all FDIC locations, it provides a mechanism to facilitate the procurement of IT hardware and software resources to meet corporate goals of rapid response during emergencies. The services that are required under this TO are a critical component of FDIC's capability to respond to banking surge activities in a timely and secure manner.

Additionally, FDIC currently has an Information Technology Application Services (ITAS) contract that provides the application services needed to support the development and maintenance of applications for the primary lines of business: insurance and supervision, receivership and operations, and mission support/strategic resources management. The ITAS contractors provide third-tier help desk services to assist in the resolution of incident and problem tickets for the applications that they build and maintain. The ITAS contract is separate from ISC and is scheduled to expire in March 2015.

#### **C.1.1 PURPOSE**

The purpose of this ISC procurement is to support the FDIC, DIT, Infrastructure Services Branch (ISB) in providing full IT infrastructure support. This TO shall provide a single point of accountability to produce innovative, efficient, and cost-effective IT infrastructure support services and to align infrastructure management and support with industry best practices. The TO requirements shall be incentivized through the use of a performance-based contracting structure (**See Award Fee Plan Section J, Attachment C and Service Level Metrics Section J, Attachment D**).

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.1.2 AGENCY DIT/ISB MISSIONS

The FDIC DIT's mission is to provide innovative, timely, reliable, and secure IT services to the FDIC. This is done by providing business value through their understanding, knowledge communications, agility, and commitment to customer service. The ISB mission is to ensure DIT provides a highly available IT infrastructure for the FDIC. The FDIC's DIT provides and maintains the technologies required to support the FDIC's mission of preserving and promoting public confidence in the United States (U.S.) financial systems through the insurance of deposits in banks and thrift institutions. DIT is comprised of logically organized teams that focus on the business and operational aspects of ensuring the right technology and associated services are available for the continued success of the FDIC.

The FDIC DIT is the organization within the FDIC responsible for providing enabling technologies and services that improve the way the FDIC accomplishes their business in a reliable, secure, and cost effective manner. Within DIT are four branches and an IT Security and Privacy Staff function (See **Section C.1.3** below). The ISB is the office with life cycle responsibility for FDIC's telecommunications, voice, video, mainframe, and server operations. Additionally, ISB has responsibility for nationwide help desk and asset management responsibilities for the FDIC.

Within DIT, the ISB is chartered with providing the underpinning infrastructure technologies that are the enabling platform for IT capabilities. Today, the ISB organization is focused on modernizing the infrastructure used by, and the services provided to, ISB clients. This modernization effort is aimed at driving out inefficient processes and deploying technologies that improve the reliability and adaptability of the environment. From a service management perspective, ISB is in the early stages of developing enterprise-wide management processes to support this modernization effort.

### C.1.3 ORGANIZATIONAL STRUCTURE

The FDIC DIT is comprised of five functional areas providing services that cross FDIC organizational boundaries. These five areas include four branches and one staff office: Enterprise Technology Branch (ETB), Delivery Management Branch (DMB), Business Administration Branch (BAB), ISB, and the Information Security and Privacy Staff (ISPS) office. ISPS has a direct reporting relationship to the FDIC Chief Information Officer (CIO). ISB is the responsible organization for the primary oversight and technical direction within this TO, with ISPS providing oversight for security operations.

The ISB is organized into five sections as well. Those sections are:

- a. **Operations:** Responsible for the daily operations of the technical infrastructure, including access control security operations, the mainframe, mid-range (Unix), Windows Intelligence (WINTEL), telecommunications, desktop and wireless platforms, and help desk support.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- b. **Infrastructure Management:** Responsible for ensuring the asset management and procurement of IT hardware/software assets, capacity management, configuration management, and infrastructure contracting programs are effective for the FDIC. This section also coordinates with FDIC Facilities, Division of Administration (DOA) for all infrastructure support as it relates to building/office moves and relocations, heating, ventilation, and air conditioning (HVAC), and other environmental needs as it relates to the infrastructure.
- c. **Engineering:** Responsibilities include review, analysis, design, architecture, engineering, configuration, testing, and deployment of hardware, software, and office connectivity throughout the FDIC.
- d. **Development and Engineering Support:** Responsibilities include oversight of the development and laboratory environments, including application development support. Additional responsibilities include testing hardware and software configurations developed by engineering prior to operational release.
- e. **Client Services (Washington, DC, Atlanta, Chicago, Dallas, Kansas City, New York, and San Francisco):** Responsibilities include the development, implementation, and compliance with plans, policies, and standards established by FDIC Headquarters. Client Services also serves as a liaison between clients and DIT regional and headquarters staffs.

The ISPS is responsible for providing enterprise-wide information security and privacy programs that ensure integrity, confidentiality, and availability of corporate information by proactively protecting the assets from unauthorized access and misuse.

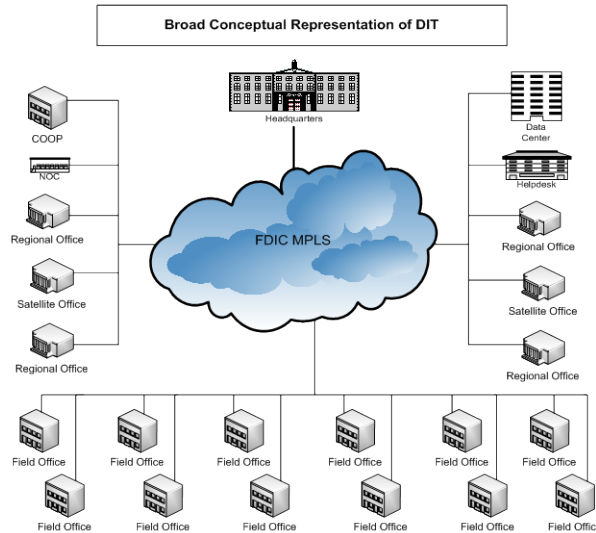
### C.1.4 **FDIC SITES**

The contractor shall support users at FDIC Headquarters and regional, satellite, and field sites as identified in **Section J**. This number will decrease by approximately 400 users by the April 2014 with the closing of one satellite site in Jacksonville, Florida.

### C.1.5 **DIVISION OF INFORMATION TECHNOLOGY**

The following represents DIT's organizational relationship to FDIC Headquarters and the regional, satellite, and field sites.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK



### C.2 SCOPE

The contractor shall perform the tasks outlined below in support of the FDIC, DIT, and ISB organizations on a performance-based basis following Government-provided service level metrics (**See Section J, Attachment D**). These tasks support the daily operations of the organizations as well as major initiatives that help DIT/ISB to standardize the IT environment and increase efficiency and effectiveness and help FDIC/DIT/ISB achieve its objective/vision. The Government has space for contractor personnel available, as indicated in **Section H.5**; however, the contractor may provide solutions that are not in Government facilities for all functionalities except the data center. The primary data center will remain in a Government facility. The contractor may provide any combination of on- or off-site approaches within the contractor personnel space constraints described in **Section H.5**. The contractor shall provide space for all support that cannot be accommodated within the Government-provided space. All Government-provided servers will be located in Government space. The Government will provide communication capability to the servers as appropriate to the contractor's solution. All Government-provided infrastructure items are Government-owned and shall be contractor maintained.

Long-distance travel is anticipated in support of these requirements for specialized installations and trouble shooting and for relocation of offices. There is no regularly scheduled long-distance travel.

Contractor personnel are required to work on site at the primary data center in the FDIC Headquarters at Virginia Square in Arlington, Virginia and in the following sites. Core hours of operation are from 6:00 AM to 8:30 PM ET. The following are the historical numbers of full-time equivalent (FTE) contractor personnel that are on-site at regional offices:

Atlanta, GA:	1 FTE
Boston, MA:	1 FTE

Contract Number GS00Q09BGD0025  
Task Order GST0013AJ0084  
Modification PO12

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

Chicago, IL:	1 FTE
Jacksonville, FL:	6 FTEs (satellite site consisting of 5 FTE Help Desk (HD)/Tier 2, 1 Telecomm) <i>Scheduled for closure in April 2014.</i>
Dallas, TX:	15 FTEs
San Francisco, CA:	1 FTE

Most other on-site support in the field and regional offices is provided by Government personnel, unless specialized assistance is needed. See **Section J, Attachment III** for the number of FDIC users by city.

The number of bank closings has decreased over time as can be seen below. This trend is expected to continue.

2012: 51 closings  
2011: 92 closings  
2010: 157 closings  
2009: 140 closings  
2008: 25 closings

The Government estimates there will be less than 20 bank closings for Calendar Year 2013.

### **C.3 VISION AND OBJECTIVE**

The FDIC's guiding vision is to provide the solution in terms of the FDIC's IT Service Agreement Vision Document (See **Section J, Attachment BBB**). Within this guiding vision, the FDIC wishes to evolve the enterprise architecture by simplifying the IT environment to ensure stable and cost-effective performance for mission-critical applications; by enhancing current security and privacy programs to work toward addressing and mitigating the new and evolving risks to sensitive data; and by establishing and monitoring IT baselines and metrics, reviewing costs, and managing service level metrics.

DIT desires to always exceed customers' expectations by providing innovative, timely, reliable, and secure IT services to FDIC. In support of this desire, ISB has adopted a vision to guide decisions in the identification, implementation, and support of infrastructure capabilities. ISB desires to constantly evaluate established and emerging technologies for alignment to FDIC business requirements, and select and implement those technologies that present the best value combination of capability, supportability, flexibility, and cost.

### **C.4 CURRENT INFORMATION TECHNOLOGY (IT) ENVIRONMENT**

The current IT environment can be found in the attachments contained in **Section J.1**.

All servers (See **Section J, Attachment X**) are less than five years old. The servers are used virtually such that applications and processing moves between servers.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5 TASKS

FDIC experiences some seasonal variation in support requirements for end-of-year processing and procurements and for asset inventory management. FDIC's fiscal year is based on the calendar year.

The contractor shall support the following task areas:

- Task 1: Enterprise Management Services (EMS)
- Task 2: Enabling Technology Services (ETS)
- Task 3: Client Support Services (CSS)
- Task 4: Protection Assurance Services (PAS)
- Task 5: Engineering and On-Demand Services (EODS)
- Task 6: Development, Quality Assurance/Testing Support
- Task 7: Asset Acquisition Services (AAS)

#### C.5.1 TASK 1: ENTERPRISE MANAGEMENT SERVICES (EMS)

Enterprise Management Services (EMS) is an approach for instilling a holistic, cross-technology and capability management function. Aimed at promoting an enterprise view of all service provisioning within FDIC, a successful implementation of EMS will eliminate stove-piped service delivery, maximize the end-user experience in using FDIC IT services, and create a mindset that strives for continuous improvement in all aspects of IT capability. It is critical that contractor and FDIC leadership jointly pursue these goals and collaboratively identify and evaluate opportunities.

The contractor's role in EMS is twofold. First, the contractor shall act as a source of industry expertise and as a catalyst in establishing necessary processes and procedures. Alignment to industry standards (such as Information Technology Information Library (ITIL) and Control Objectives for Information and Related Technologies (COBIT) will provide the underpinning of the EMS, and the contractor shall provide that expertise. Second, the contractor shall provide the tactical oversight of implementation and on-going management. The contractor shall provide continuous monitoring of EMS success and make adjustments, where required, to ensure achievement of goals and maintenance of service.

The Government will provide governance procedures and practices (**See Section J, Attachment B**) in order to facilitate a productive relationship between FDIC and the contractor. The contractor shall comply with these governance procedures (**See Section J, Attachment A**).

The contractor shall provide the support described in the following sections.

- a. Program Management, to include invoicing and financial management
- b. Enterprise Control Processes
- c. Infrastructure Architecture and Infrastructure Standards

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- d. Disaster Recovery / Business Continuity
- e. Performance Management
- f. Reporting
- g. Asset Management
- h. Training
- i. Technology Innovation
- j. Transition Support

The contractor shall support the Government in its implementation of ITIL best practices by assisting with aligning and integrating FDIC's current ITIL frameworks. Also, FDIC systems are frequently audited, and the contractor shall provide information in support of these audits. The Chief Financial Office Auditor (CFOA), in particular, uses the COBIT 5 framework as a measuring tool for their audits.

### **C.5.1.1 PROGRAM MANAGEMENT**

#### **C.5.1.1.1 PROGRAM MANAGEMENT PLAN (PMP)**

The contractor shall develop and deliver a Draft and Final PMP (See Section F, Deliverable 01 and 02) that is based on the contractor's proposal for transition and all task areas. The contractor shall provide PMP Updates (See Section F, Deliverable 03) throughout the TO performance period. At a minimum, this PMP shall include:

- a. All technical activities (including documentation development) identified and organized in a Work Breakdown Structure (WBS) at a level of detail sufficient for the contractor to manage the work at no less than at a week by week basis. At a minimum, the WBS shall be broken down at the task level. The contractor shall prepare the WBS in Microsoft Project.
- b. The contractor's technical, management approach, Quality Control Plan (QCP) tailored to the FDIC requirements, and associated responsibilities and partnerships between or among Government organizations.
- c. An Action Item Log.
- d. A Gantt chart that contains activities and milestones pertinent to the contractor's completion of the technical activities.
- e. All performance standards followed in support of these requirements.
- f. A description of expected result of each WBS level or milestone in the Gantt chart.
- g. A matrix of all deliverables, their version/release, and planned delivery dates.
- h. Status of current and planned initiatives and programs.
- i. Task dependencies and interrelationships.
- j. The contractor's organizational structure.
- k. Process management and controls.
- l. Any unique hardware and software utilized by the contractor.
- m. A description of the application(s) used to monitor the performance of the network.



## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.1.1.2 PROGRAM MANAGEMENT BRIEFINGS/MEETING/REPORTS

- a. The contractor shall schedule and coordinate a Project Kick-Off Meeting (**See Section F, Deliverable 04**) at the FDIC site. At a minimum, the attendees shall include the contractor's Key Personnel, FDIC personnel, and the FEDSIM Contracting Officer's Representative (COR). The contractor shall prepare a Project Kick-off Briefing (**See Section F, Deliverable 05**) and discuss the following, at a minimum:
  1. Schedule
  2. Service-level metrics
  3. Security requirements
  4. Government-furnished information
  5. Monthly meeting dates
  6. Points of contact
  7. Task order transitioning process and timeframes
  8. Prioritization of contractor activities

The contractor shall prepare a Project Kick-off Agenda (**See Section F, Deliverable 06**) that includes, at a minimum, the above referenced items.

- b. The contractor shall attend and participate in executive briefings to be conducted, at a minimum, quarterly. Such briefings shall focus on contractor performance against service-level metrics, open issues in the delivery of services, and other items desired by FDIC executives and program leadership.
- c. The contractor shall plan, schedule, and conduct Biweekly PMO Meetings (**See Section F, Deliverable 07**) with the FDIC Oversight Manager, FEDSIM COR, and other FDIC named stakeholders. The meeting agenda shall focus on the status of services delivery, project activities, the status of all outstanding issues, and progress toward metric compliance and satisfaction. FDIC program leadership may alter meeting agendas when required to address specific issues related to the delivery of services.
- d. The contractor shall prepare Meeting and Review Minutes (**See Section F, Deliverable 08**) for meetings and reviews that relate to the TO scope where the contractor is in attendance. At a minimum, the minutes shall contain the following:
  1. Date and place
  2. Attendees
  3. Purpose of meeting/review
  4. Brief description of items discussed
  5. Results
  6. Action items

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- e. The contractor shall attend and actively contribute to objectives of meetings for projects, design reviews, change control boards (CCB)/reviews (ISB – CCB (twice per week) / DMB – PRR (weekly) tiger teams (average one to four per week), daily infrastructure, weekly oversight with team leads, audits (four per year), and operations manual review meetings. The contractor shall also participate in a daily operations meeting, ERB (once a week), the TRG (one a month), biweekly PMO, biannual technical refresh, quarterly service-level metrics reviews, and quarterly self-assessments.
- f. The PMB is the governing board for DIT/BAB/IMS procurements. The purpose of the PMB is to ensure that FDIC budgetary resources for hardware, software, and other non-labor IT items are expended in a planned and orderly manner. The purpose and content discussed during this meeting may evolve as FDIC needs change. The contractor shall provide the following PMB information, at a minimum:
  1. Procurement Activity Report to include: monthly and Year to Date (YTD) and comparison to previous year
  2. Unscheduled Procurements Report
  3. AAS Audit Report
  4. AAS Process Review Report
  5. Outstanding Quarterly Recurring Procurement Status Report
  6. Metrics associated with the following:
    - i. Bill of Material (BOM) Information
      - Number of maintenance and services BOM's to be prepared for the period and estimated acquisition value
      - Number of maintenance and services BOM's prepared and submitted to the FDIC for processing and estimated acquisition value
      - Number of unplanned BOM's prepared and submitted to the FDIC for processing and estimated requisition value
    - ii. Non-Trade Agreement Act (TAA) Information
      - Number of non-TAA compliant related waivers prepared for the period for submission to the FDIC and estimated acquisition value
      - Number of procurements executed through the contract that did not comply with the TAA and estimated acquisition value
  7. Cost Savings Report
  8. YTD Top Vendor Procurement Activity Report
    - i. By dollars
    - ii. By count
    - iii. Approved recurring procurement report
  9. Forecasting information from the Quarterly Spend Plan
    - i. Section 508 Compliant Information
      - Number of Voluntary Product Accessibility Templates (VPAT) planned for maintenance and services prepared during the period
      - Number of VPAT's for maintenance and services prepared and submitted to the FDIC for processing

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- Number of VPAT's for maintenance and services not prepared, rationale for non-preparation, and estimated acquisition value
  - ii. Energy Star and Electronic Product Environmental Assessment Tool (EPEAT) Information for all electronic goods purchased through the contract and associated acquisition value
- g. The Government will provide the format and expected content for the Monthly Performance Report to be provided by the contractor. Such content and format will be determined at project start and reviewed at least every six months by the FDIC Oversight Manager for applicability and any necessary modifications. The contractor shall develop and provide a Monthly Performance Report (**See Section F, Deliverable 09**) by the 10<sup>th</sup> business day of the month that succinctly summarizes the management and technical progress to date including the following, at a minimum:
  - 1. Management status by task area
    - i. Accomplishments
    - ii. Issues and risks
    - iii. Areas for improvement, efficiencies, or innovation
    - iv. Meetings
    - v. Performance standards in danger of not being met and mitigation actions
  - 2. Reports and deliverables completed in the past month.
  - 3. Personnel gains, losses, and status (security clearance, etc.).
  - 4. Government actions required.
  - 5. Financial summaries, to include but not limited to, procurement tracking reports, monthly accrual report, monthly financial report, and monthly spend plan.
  - 6. Monthly Key Performance Indicator (KPI)/Operational Performance Indicator (OPI) scores, to include:
    - i. Listing of all KPI/OPI
    - ii. All data driving KPI/OPI measurements
    - iii. Detailed performance to each KPI/OPI metric
    - iv. Summary of Pass/Fail
    - v. Each quarterly (per FDIC budget year – calendar year) provide trending of KPI/OPI compliance for the past four quarters
- h. The Contractor shall submit a Monthly Financial Report, (**See Section F, Deliverable 10**) that provides the FDIC with a summary of contract spending (by CLIN) to include, at a minimum:
  - 1. Projected spending (current month, year-to-date)
  - 2. Actual spending ( current month, year-to-date, contract inception-to-date)
  - 3. Estimated Incurred (Accruals and in-process)
  - 4. Burn Rate & Staffing Rate
  - 5. Variances (dollar amount, percentage)
  - 6. Detailed break-down (labor categories, non-labor)

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

7. Narrative describing variances greater than 5 percent (+/-), cost savings, and cost related issues
- i. The Contractor shall submit a Monthly Accrual Report (**See Section F, Deliverable 11**) that provides FDIC with a summary of all contract expenses incurred but not invoiced for the current month and a cumulative amount to date for each year of the TO.
- j. The Contractor shall submit and maintain a Quarterly Spend Plan (**See Section F, Deliverable 12**) that reflects projected spending for the upcoming 12 months. This shall include a detailed breakout by the following:
  1. Reports and deliverables completed in the past month
  2. Personnel gains, losses, and status (security clearance, etc.).
  3. Government actions required.
  4. Financial summaries, including, but not limited to, procurement tracking reports, monthly accrual report, monthly financial report, and monthly spend plan
  5. Monthly Key Performance Indicator (KPI)/Operational Performance Indicator (OPI)
  6. CLIN
  7. Labor costs by labor category
  8. Travel spending
  9. Ancillary products and/or services (e.g., hardware, software, and maintenance/license agreements)
  10. Projects

### C.5.1.1.3 PROGRAM MANAGEMENT WEB PORTAL

The contractor shall provide a Program Management Web Portal Design (**See Section F, Deliverable 13**) that makes use of the existing FDIC portal infrastructure and software that is SharePoint based and is integrated with the FDIC-required reporting system within 30 calendar days of Project Start (PS). After Government approval of the portal design, the contractor shall develop and implement the Program Management Web Portal (**See Section F, Deliverable 14**). The portal shall be reviewed semi-annually by FDIC for appropriateness and functionality. The contractor shall provide Program Management Web Portal Updates at least annually. See **Attachment MMM** for the functionality of the current web portal. The contractor shall design additional report generation within the current design.

### C.5.1.2 ENTERPRISE CONTROL PROCESSES

The contractor shall provide an Enterprise Control Process Implementation Plan (**See Section F, Deliverable 15**) consisting of a comprehensive, integrated set of tools, processes, and procedures that shall migrate the FDIC IT functionality into a satisfactory level of alignment with ITIL, Federal Information Security Management Act (FISMA), and COBIT guidelines. All hardware and software will be provided by the Government or purchased through the TO. The contractor

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

shall implement the Plan after receipt of Government approval. The contractor shall provide the following in the Plan, at a minimum:

- a. Necessary process and procedure changes from current FDIC actions
- b. Necessary tooling (software, hardware) to be implemented
- c. Levels of leverage of existing FDIC tooling
- d. Awareness and inclusion of FDIC security requirements in all process design and execution
- e. Interfacing groups required for alignment
- f. Workflows and process descriptions
- g. Project plans for implementation
- h. Component processes (as listed and described below)

- 1. Capacity Management
- 2. Change Management
- 3. Configuration Management
- 4. Demand Management
- 5. Financial Management
- 6. Incident Management
- 7. Problem Management
- 8. Release Management
- 9. Enterprise Control Process Oversight
- 10. Documentation
- 11. Other processes as proposed by the contractor

- i. **Capacity Management:** The contractor shall assess the current processes for alignment to FDIC needs, propose any enhancements or changes, and implement a Capacity Management Process that provides a single focus of management for all capacity and performance-related issues. For a list of items that the Capacity Management Process shall include at a minimum, see **Attachment MMM**.
- ii. **Change Management:** The contractor shall assess the current processes for alignment to FDIC needs, propose any enhancements or changes, and implement a Change Control and Management Process that provides the necessary level of oversight, review, and approval for all changes required in the FDIC IT environment. For a list of items that the Change Control and Management Process shall include at a minimum, see Attachment MMM.
- iii. **Configuration Management:** The contractor shall assess the current processes for alignment to FDIC needs, propose any enhancements or changes, and implement a Configuration Management Process that enables a logical model of the IT environment to be viewed by the individual components and component aggregations that make up the IT services. See Attachment MMM for a list what the Configuration Management Process shall include, at a minimum.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- iv. **Demand Management:** The contractor shall assess the current processes for alignment to FDIC needs, propose any enhancements or changes, and implement a Demand Management Process for FDIC, in conjunction with the contractor, to reliably forecast changes in demand for services and the IT infrastructure components. See Attachment MMM for a list of what the Demand Management Process shall include at a minimum.
- v. **Financial Management:** The contractor shall assess the current processes for alignment to FDIC needs, propose any enhancements or changes, and implement a Financial Management Process that provides FDIC IT leadership the desired level of visibility to financial information about IT services that is accurate and timely. See Attachment MMM for a list of what the Financial Management Process shall include, at a minimum.
- vi. **Incident Management:** The contractor shall assess the current processes for alignment to FDIC needs, propose any enhancements or changes, and implement an Incident Management Process that defines the approach and processes used by all support teams in the identification, tracking, investigation, resolution, and documentation of any service request presented by an FDIC IT end user. See Attachment MMM for a list of what the Incident Management Process shall include, at a minimum.
- vii. **Problem Management:** The contractor shall assess the current processes for alignment to FDIC needs, propose any enhancements or changes, and implement a Problem Management Process that actively identifies and remediates repetitive incidents or identifies likely service delivery issues and remediates them in advance. See Attachment MMM for a list of what the Problem Management Process shall include, at a minimum.
- viii. **Release Management:** The contractor shall assess the current processes for alignment to FDIC needs, propose any enhancements or changes, and implement a Release Management Process that defines the evaluation and planning processes required to ensure FDIC controlled, timely release of new capabilities, principally in software, into the FDIC IT environment. See Attachment MMM for a list of what the Release Management Process shall include, at a minimum.
- ix. **Enterprise Control Process Oversight:** The contractor shall perform continual oversight of adherence to Enterprise Control Process requirements by all DIT-related contractors and FDIC personnel.
- x. **Documentation:** The contractor shall provide Standard Operating Procedures (SOP) for all operational and management tasks performed, workflows and process diagrams for all service desk incident handling process, and enterprise management

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

process documentation for the initiation, maintenance, and execution of each enterprise management process.

### **C.5.1.3 INFRASTRUCTURE ARCHITECTURE AND STANDARDS SUPPORT**

The Government will provide the FDIC strategies and infrastructure architectures and an infrastructure standards definition that complies with FDIC Policy and Guidelines. FDIC's draft business technology strategic plan 2013-2017 is provided, **see Attachment E**. The Government will also appoint an Infrastructure Architecture Lead for the FDIC IT environment with whom the contractor shall interface.

#### **C.5.1.3.1 INFRASTRUCTURE ARCHITECTURE DEVELOPMENT SUPPORT**

The contractor shall proactively contribute to the development and maintenance of infrastructure architectures for the FDIC IT environment. The contractor shall lead the translation and estimation of architectural directions into support requirements, including impact on current support operations and capabilities, risk analysis of proposed migrations, and supportability of new technologies. In addition, the contractor shall assist FDIC with identifying and connecting with industry Original Equipment Manufacturers (OEMs) and technology leaders. The contractor shall also assist in Governance and performance management actions aimed at identifying infrastructure architecture and technology needs and improving performance of FDIC IT capabilities. Finally, the contractor shall assist FDIC with strategy formulation through discussions and conducting research related to infrastructure architecture.

#### **C.5.1.3.2 INFRASTRUCTURE STANDARDS SUPPORT**

The contractor shall assist FDIC with IT infrastructure standards development, in moving toward standard configurations across the entire organization, and documenting and maintaining infrastructure standards. In addition, the contractor shall assist the FDIC infrastructure architecture group in communicating infrastructure standards to FDIC personnel and participate with FDIC representatives on permanent and ad-hoc committees and working groups. The contractor shall research, design, and recommend processes to achieve standardization of the services, and technical solutions based on business needs, third-party contractor products and services, and infrastructure requirements.

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

### **C.5.1.3.3 LONG-RANGE SYSTEM PLANNING**

The contractor shall evaluate and recommend appropriate tools and processes that enhance the stability and functionality of the environment, and allow provision of services in accordance with FDIC's Infrastructure Architecture and Infrastructure Standards, and the service levels. The contractor shall also assist FDIC with long-range system plans by providing the following services, at a minimum:

- a. Compare and assess requirements against the current installed Infrastructure Architecture, as well as the future Infrastructure Architecture, as defined by FDIC IT, to assess the impact on the IT infrastructure for satisfying these requirements.
- b. Participate with FDIC representatives on permanent and ad-hoc committees and working groups addressing such issues.
- c. Identify opportunities to consolidate devices and services, utilize new technologies, and improve the delivery of services.

### **C.5.1.4 DISASTER RECOVERY/BUSINESS CONTINUITY SUPPORT**

The Government will provide its overall Disaster Recovery and Business Continuity Plans, including FDIC assets and locations (**See Section J.1**), management of the Disaster Recovery sites (FDIC and/or contractor), and testing of the Disaster Recovery/Business Continuity Plans. The Government has transitioned to a new disaster recovery site in Manassas, Virginia. This was completed in July 2012. The contractor shall support the systems remotely and on occasion shall provide on-site support to update equipment and/or support disaster recovery activities. The Government will provide a space for staging and smart hands (remote-servicing) support. The FDIC envisions this new disaster recovery site will evolve to a business Continuity of Operations (COOP) site and then to a site synchronized with the FDIC headquarters site. See **Section J, Attachment FF** for disaster recovery site inventory. The contractor shall support this site as a lights-out, co-located site and provide the following planning and management support.

#### **C.5.1.4.1 DISASTER RECOVERY PLANNING SUPPORT**

The contractor shall review existing plans, make recommendations, and incorporate FDIC-approved changes to Disaster Recovery/Business Continuity Plans (**See Section F, Deliverable 17**). The plans shall restore FDIC-identified infrastructure mission critical functionality in the event of a disaster and to maintain business continuity of such functionality. The contractor shall provide separate plans for FDIC assets and locations, and contractor assets and locations. For a list of what the Disaster Recovery/Business Continuity Plans shall include, at a minimum, see **Attachment MMM**.



## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### **C.5.1.4.1.1 DISASTER RECOVERY PLANNING SUPPORT (FROM A CONTRACTOR FACILITY)**

For services delivered from a contractor facility and for all tooling implemented in the FDIC IT environment provided by the contractor, the contractor shall provide planning and implementation of contingency and disaster recovery processes to meet the services availability requirements. The contractor shall also update and maintain the currency of disaster recovery and business continuity plans and procedure manuals as changes to infrastructure, applications, and business needs are made or identified. For a list of what the disaster recovery support for a contractor facility shall include, at a minimum, see **Attachment MMM**.

### **C.5.1.4.1.2 DISASTER RECOVERY PLANNING SUPPORT (FROM AN FDIC FACILITY)**

The contractor shall update and maintain the currency of disaster recovery and business continuity plans and procedure manuals as changes to infrastructure, applications, and business needs are made or identified to include. For a list of what the disaster recovery support for a contractor shall include, at a minimum, see **Attachment MMM**.

### **C.5.1.4.2 DISASTER RECOVERY MANAGEMENT**

The contractor shall provide disaster recovery management remotely, unless repairing or replacing equipment. The contractor shall help define recovery requirements, perform recovery activities, and coordinate disaster recovery efforts. Also, the contractor shall develop, maintain, and publish a notification and escalation process for FDIC approval on actions to occur when a disaster or any interruption to normal operations is experienced or suspected. Finally, the contractor shall provide crisis management support (**See Attachment MMM**).

The contractor shall lead and execute testing of disaster recovery and business continuity plans in accordance with requirements provided by the Security Policy and Compliance organization leadership. Currently, testing of half of the system is done by the contractor twice a year. This constitutes full testing of the system every year. For a list of procedures associated with disaster recovery testing, (see **Attachment MMM**).

### **C.5.1.5 PERFORMANCE MANAGEMENT**

The contractor shall work cooperatively with FDIC to ensure all performance management processes and procedures support the open sharing of information and honest dialogue in the investigation of performance issues. The contractor shall leverage its industry experience and expertise in recommending, implementing, and operating industry best practices. The contractor shall propose changes and implementations to the FDIC. The contractor shall include anticipated benefits, costs to implement, and a timeline. Key among the industry best practices that offers proven and predictable outcomes is the ITIL. FDIC is currently developing its understanding of this set of processes through training and certification of personnel in the application of the

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

management processes. The contractor shall participate in this activity. Specifically, the contractor shall actively participate in the development of the following, at a minimum.

- a. A service catalog for all services.
- b. A review plan for all Enterprise Management Processes (e.g., change control processes and configuration management) for needed changes to reach compliance with ITIL standards.
- c. Management communications for disseminating planned actions.

### **C.5.1.5.1 ENTERPRISE PERFORMANCE MANAGEMENT APPROACH**

The contractor shall develop and maintain an Enterprise Performance Management Approach (See Section F, Deliverable 18) that leverages enterprise management control problem management processes in identifying and resolving problems. The Enterprise Performance Management Approach shall achieve the following items, at a minimum.

- a. Leverages enterprise management control problem management processes in identifying and resolving problems.
- b. Focuses on ensuring FDIC achieves continual value from contractor services and the FDIC IT capabilities.
- c. Proactive in the identification and remediation of issues that will impact the successful use of FDIC IT infrastructure components and capabilities.
- d. Reactive to IT environment incidents and problems in a controlled, predictive manner that alleviates the occurrence and end-user impact, while identifying ways to reduce the threat of reoccurrence.
- e. Proactively addresses performance issues in the FDIC IT environment.
- f. Triangulates capacity, utilization, demand planning, performance, and other data sources in predictive analysis of environment performance issues.
- g. Combines contractor and FDIC support resources in the identification, investigation, and resolution of performance issues in the environment, particularly those that cross technological and support team boundaries.
- h. Provides a level of technical and performance skills to understand and propose needed optimization and issue resolution solutions in the following categories:
  - 1. Server / hosting technologies (to include Unix, Wintel, and virtualization)
  - 2. Mainframe technologies
  - 3. Storage technologies (to include network, direct attached, and Storage Area Network (SAN) options)
  - 4. IT operational processes
  - 5. Web enablement
  - 6. IT security and protection technologies
  - 7. Networking technologies (to include Wide Area Network (WAN)/ Local Area Network (LAN) / telephony/video)
  - 8. End user workstations (desktops, laptops, printers, scanners)
  - 9. Remote Access

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

### **10. Current and emerging industry implementations and adaptations**

#### **C.5.1.5.2 SERVICE DEMANDS**

Throughout the TO, the potential exists for FDIC to request a re-prioritization of service actions that will be coordinated with a reprioritization of award fee as appropriate. All such re-prioritizations will be approved by the FDIC.

Unplanned service needs are support tasks required to meet the IT needs of the FDIC business that are not codified in the services contract. These needs may be new in nature, driven by the evolving makeup of the IT environment, or omissions made in the initial service definitions that make up the services agreement.

FDIC expects these unplanned service needs to arise and will require cooperation and resource utilization by the contractor. Many such service needs will require immediate and concerted attention to avoid potential negative affects to FDIC or FDIC customers. For unplanned service needs that require incremental resource hours, FDIC and the contractor will use the Change Control Process to evaluate the costs of the service need and the contractor shall propose costs as part of the evaluation.

In requests for support for unplanned service needs, the contractor shall, when requested by FDIC, immediately commence support activities in parallel with discussions on the size of the request and any compensation or relief to be granted.

All such requests for unplanned service needs will be approved by the FDIC IT Services Oversight Manager or named designee in writing or email.

In an IT environment with the breadth and depth of uses and technologies as FDIC's, the need for immediate, extraordinary support effort will occasionally arise. Such needs may be driven by a security breach in the networks, a viral infection in a desktop image, a severe outage of a critical system, or other such events.

Such support efforts will require the dynamic forming of rapid response teams to work closely with FDIC and other FDIC contractors to immediately identify the underlying cause of the emergency, work to eliminate or mitigate the impact, and seek ways to prohibit or minimize the reoccurrence.

#### **C.5.1.5.3 PERFORMANCE MANAGEMENT OF INCIDENTS**

The contractor shall investigate and determine the underlying cause, and, where appropriate, repair all performance problems that occur in the delivery of the services. Problems may be recognized as the result of notification to the service desk, the activation of a monitor, or contractor, third-party contractor, or FDIC alerting systems.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

Participation in resolving incidents, regardless of their source, is a key element of contractor's performance. As such, the contractor shall adhere to FDIC Policies and Procedures for incident logging and documenting incidents, participate in severity Incident Resolution Bridges (IRBs), and perform and support the RCA processes. An IRB is a conference call that is established by the contractor to coordinate the resolution of selected Incidents.

If the contractor is unable to meet the required performance standards the contractor shall, at a minimum.

- a. Immediately notify the FDIC Technical Monitor, detailing the incident, the required actions, and the noted deficiency of other organizations.
- b. Employ existing OPIs to escalate the issue within the deficient organization's management chain.
- c. Using reasonable efforts and continue attempts necessary to reach problem understanding and resolution.

### **C.5.1.5.3.1 INCIDENT MANAGEMENT**

The contractor shall document all incidents in the incident management ticketing system that are implemented and maintained at the service desk. The contractor shall open, monitor, and manage all open incident tickets regardless who is responsible for the resolution of the ticket. See **Attachment MMM** for a list of minimum procedures for all incidents, incidents where the resolution is the responsibility of the contractor, and incidents where resolution is not the responsibility of the contractor and upon recognition of a deficiency, outage, or degradation of a capability in the IT infrastructure.

### **C.5.1.5.3.2 INCIDENT RESOLUTION BRIDGE (IRB)**

For all non-VIP Severity 1 Incidents, the contractor shall establish an IRB for ensuring all affected parties and appropriate levels of FDIC IT management are appraised of the incident, actions underway to investigate the incident, and anticipated resolution times (**See Section J, Attachment EEE** for the number of current VIP members by location). This bridge will consist of a toll-free telephone conference line, and the conference will be attended by designated persons from FDIC, the contractor, and all third-party contractors pertinent to the incident. For a list of minimum procedures associated with the IRB, see **Attachment MMM**.

The contractor shall ensure the appropriately skilled and empowered personnel are in attendance on IRBs to provide technical input into the incident investigation.

### **C.5.1.5.3.3 ROOT CAUSE ANALYSIS (RCA)**

Certain incidents will require that an RCA be performed in an attempt to understand the underlying problem(s) that triggered an incident or allowed it to occur. The contractor shall, at a minimum, conduct an RCA for all Severity 1 failures, missed service levels, and at the request of

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

the FDIC Technical Monitor. The FDIC Technical Monitor may request such analysis for any incident.

The contractor shall perform RCA for those incidents that were the contractor's responsibility to resolve, and participate in and support the RCA process for other incidents where requested by the FDIC Technical Monitor. For a list of processes and techniques associated with RCA activities, see **Attachment MMM**. All RCA investigations, solutions, and implementations shall be reported to FDIC in compliance with the particular service area reporting requirements. The contractor shall provide the Service Area Reports (See **Section F, Deliverable 33**) described in **Section J, Attachment G**

### **C.5.1.6     TASK/SERVICE AREA PROJECT REPORTING**

The contractor shall provide project reporting in accordance with the following overarching functionality. See **Section J, Attachment G** for the minimum contents of specific reports listed in each Task/Service area). The contractor shall provide changes to the reports and/or create and publish new reports in accordance with the change control processes.

- a. On-Demand (OD) Generation Reports shall be available for generation or access by selected FDIC personnel when desired by accessing contractor's network-based reporting system and requesting the report. For a list of what the OD Generation Reports shall include, but are not limited to, see **Attachment MMM**.
- b. Scheduled Delivery (SD) Reports shall be formatted for mass distribution and delivered through the FDIC email system to a publishing list established by the FDIC Enterprise Governance Council, or their designees, and the FEDSIM COR. Scheduled Delivery Reports will also be available as On-Demand Generation Reports, in accordance with the above requirements, for those Authorized Users with access to the reporting system.
- c. The contractor shall provide, implement, configure, and maintain a web-based system for collecting, tracking, and analyzing the data necessary to produce all required reports. Reports shall be developed and available to FDIC in electronic format. The reporting system shall be aligned with all performance management activities to support KPI/OPI development and management and service level accounting and compliance. In addition, the reporting system shall provide inputs to performance investigation and problem management efforts. The reporting system shall be maintained in an online repository for the duration of the TO. See **Attachment MMM** for a list of minimum requirements for the reporting system.

### **C.5.1.7     ASSET MANAGEMENT**

The Government will provide the Asset Management System (AMS) (hardware and software, including client licensing as needed) for use in the tracking and management of assets in the

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

FDIC IT environment and all required devices, software, database, and other maintenance support required to maintain the AMS.

### **C.5.1.7.1      ASSET MANAGEMENT SYSEM SUPPORT**

The contractor shall develop and provide an FDIC Asset Management Process Assessment (See **Section F, Deliverable 19**) of the current processes and supporting tooling implementation. For a list of what the FDIC Asset Management Process Assessment shall include, at a minimum, see **Attachment MMM**. As of December 2011, the asset inventory was 99.7% accurate. See **Section J, Attachment JJ** for Asset Management Data by location.

The contractor shall maintain and support the linkage of the AMS with the Incident Management System (IMS) to permit service desk and other personnel to establish and view relationships between assets, people, software, maintenance contracts, and services to enable advance reporting and usage of assets. The contractor shall also perform device discovery and monitoring for network, compute, and addressable devices. See **Attachment MMM** for a list of minimum requirements. The contractor shall investigate any reported rogue devices and alert the FDIC Technical Monitor or named designee of such devices to determine the location and the end user.

The contractor shall develop a Set of Asset Classifications to be used in categorizing devices tracked in the AMS. Classifications shall be tiered in three classes and three tier assignments. FDIC will participate in the creation of the classifications and may have up to 100 separate and distinct classifications. The system shall be able to distinguish between asset bundles and single assets (i.e., where an asset bundle is defined as a CPU and a set of peripherals). The contractor may recommend other definitions for an asset management process based upon industry best practices.

The contractor will audit and ensure compliance of all deployed software within the enterprise and will make remediation recommendations for non-compliant software.

### **C.5.1.7.2      ASSET RECEIPT AND DISTRIBUTION SERVICES**

The contractor shall provide services for receipt/distribution/dispatch of all IT assets (FDIC Headquarters/regional/field sites). The Government will provide facilities to house supplemental stock rooms at FDIC Headquarters and at other regional/field locations and provide packing materials and pay for shipping costs for asset distribution. The contractor shall move all assets currently housed at the Fulcrum site in Landover, Maryland (See **Attachment Z** for an inventory) to their receipt/distribution site by the end of the base period. Equipment is also housed at the DIT Distribution Center (DDC) at the FDIC Headquarters location. The amount of DDC inventory varies as assets are redistributed. Typical items that are maintained at the DDC are end-user computing devices (laptops, desktops, iPads, Blackberries, cellular phone, cellular modems, desktop printers, desktop scanners, desk telephones, projectors, etc.), major infrastructure devices (network racks, network patch panels, switches, routers, network printers,

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

servers, wide-area acceleration appliances, etc.), and minor peripherals/accessories (phone chargers, network patch cables, fiber-optic patch cables, keyboards, mice, privacy screens, private branch exchange (PBX) cards, etc.). This Government-provided space is currently at capacity. The contractor may use the DDC space for their solution and may redistribute assets according to their solution. Assets are also housed at various contractor sites in the Washington, D.C., and Regional areas. The Government will move these assets to the contractor's receipt/distribution site.

The contractor shall manage all assets in compliance with FDIC and governing bodies' regulations. The contractor shall manage the physical receipt of all IT assets from contractors and OEMs that are delivered to FDIC headquarters locations. The contractor shall also distribute DIT equipment to any FDIC location nationwide, to include preparing all items for shipment and delivery to the mailroom (currently located on the same floor with the DDC) for shipment. The Government will pay for shipping and materials. Items are only delivered to the FDIC mailroom if they are housed on FDIC property. The contractor shall maintain the general stock and spares of IT hardware, including consumables, for the FDIC at the DDC in order to meet service-level metrics. Finally, the contractor shall distribute and/or pickup assets to National Capital (NCR) locations. For minimum services and requirements associated with managing the physical receipt of all IT assets, maintaining the general stock and spares of IT hardware, and delivering assets to National Capital Region (NCR) locations, see **Attachment MMM**.

### **C.5.1.7.3      ASSET REFRESH SUPPORT**

In coordination with the FDIC, the contractor shall establish an Asset Refresh Schedule for each device classification and purchase classification. The Government will approve all changes to the schedule. In accordance with the established Asset Refresh Schedules, the contractor shall flag each device in the AMS for refresh notifications at six months and three months before the due date. Following the six-month refresh notification and prior to ordering new assets, the contractor shall confirm the refresh schedule and asset needs with the FDIC and validate the locations of planned deployments.

### **C.5.1.7.4      LICENSE RENEWAL & TRACKING SUPPORT**

In coordination with the FDIC, the contractor shall develop and provide License Renewal & Tracking Procedures (**See Section F, Deliverable 20**) for each software license and/or maintenance classification. All changes to the renewal and tracking procedures must be approved by FDIC. The contractor shall ensure that all software license transfers (e.g., the transfer of licenses during a device refresh and/or the transfer of licenses during resource attrition) are reflected in the AMS within two business days of the completion of the transfer. Each license resident in the AMS shall be flagged for renewal six months and three months prior to expiration. Following the six-month renewal notification and prior to ordering new software licenses and/or maintenance, the contractor shall confirm the renewal terms and software license needs with the FDIC. No sooner than three months before the software license and/or maintenance expiration date, the contractor shall renew the software licenses and/or maintenance

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

with FDIC and FEDSIM approval. The contractor shall understand and document the penalties for early renewal. The renewal process shall be just-in-time and include no overlap cost of the software licenses and/or maintenance. The contractor shall update the AMS with the new software license and/or maintenance expiration date(s).

### **C.5.1.7.5      MOVES, ADDS, AND CHANGES (MAC)**

Using the service desk IMS and established processes, the contractor shall track all MACs that are performed. The contractor shall ensure that all MACs are reflected in the AMS within one business day of the completion of the MAC.

### **C.5.1.7.6      DEVICE RETIREMENT SUPPORT**

In collaboration with the FDIC, the contractor shall follow FDIC documented guidelines and perform device retirements in accordance with the elements outlined in **Section J, Attachment G**. Recommendations will be provided to the Technical Monitor should changes to this documentation deem necessary. The Government will provide sanitation tools. The contractor shall conduct the sanitization and final disposition of media.

### **C.5.1.7.7      AMS AUDIT SUPPORT**

The contractor shall develop and provide an AMS Completeness Audit Process (**See Section F, Deliverable 21**) for auditing the accuracy and completeness of the AMS in accordance with the Government-approved process 60 calendar days after start of delivery of asset management services. For a list of what the process shall include, at a minimum, see **Attachment MMM**.

### **C.5.1.7.8      ASSET INVENTORY SUPPORT**

The contractor shall conduct a quarterly inventory of all software assets and develop a formal status Quarterly Inventory Report (See Section F, Deliverable 37) identifying all software assets currently installed throughout the environment; software assets legally purchased; software assets installed not purchased; software assets (over/under) subscribed based upon purchase history and installation base; and recommendations to purchase additional licenses or to de-install software not being utilized since the previous reporting period.

The contractor shall conduct a bi-annual inventory of all hardware assets and develop a formal Semi-annual Inventory Status Report (See Section F, Deliverable 38) identifying all hardware assets successfully inventoried; all hardware assets not verified during the inventory; due diligence activities conducted for and provide status for hardware assets not verified during the inventory; assets identified as surplus since the last reporting period; assets lost since the last reporting period; (assets since the last reporting period; and, assets traded-in, exchanged, or returned to vendor since the last reporting period.



## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

The contractor shall conduct a quarterly inventory of all hardware and software assets that are not under maintenance agreements and shall report each asset that is not under a maintenance agreement and rationale. (Note: the rationale might be that the equipment is being eliminated, is so old that the vendor does not offer maintenance, etc.)

The contractor shall maintain the FDIC's centralized software library to ensure that media exists for each software asset; proof of entitlement and software restrictions or usage rights exists for each software asset; proof of maintenance exists for each software asset; media installation or other security codes to install software assets exists for each software asset; and all records and media are duplicated in an offsite location for disaster recovery purposes.

### **C.5.1.8 OVERARCHING PROJECT SUPPORT**

The Government requires overarching project support on a regular basis. These projects span the service areas of the TO, and are managed in an overarching governance and controlled manner. See **Section J, Attachment CCC** for a list of current projects and their current priority for implementation.

The contractor shall work with FDIC project managers and technical leads to define business, functional, and technical requirements and scope of projects; prepare project proposals; and develop project plans, including time and line-item cost estimates, resource loading, progress to plan and percentage completion measures, and milestone and deliverable identification. See **Attachment MMM** for a list of minimum project support the contractor shall provide.

### **C.5.1.9 TRAINING SUPPORT FOR FDIC PERSONNEL**

The contractor shall provide instruction to FDIC personnel in the use, interaction with, data entry, and access methods for all tools (e.g., IMS, AMS) and support processes deployed by contractor where:

- a. Such interaction with the contractor deployed tools and processes by FDIC personnel are a required task to complete normal day-to-day tasks.
- b. Such interaction with the contractor deployed tools and processes by FDIC personnel are a required task to respond to emergency and other occurrences outside normal operations.
- c. FDIC is developing, enhancing, or maintaining other tools or support processes that interface directly or indirectly with contractor deployed tools and support processes.

The contractor shall provide training to FDIC personnel in a venue that is appropriate for the material being communicated and the size and location of intended audience. The FDIC has training facilities available. It is anticipated that the preferred training formats will be online or self-paced training. However FDIC does have training facilities available for use, if appropriate. The contractor shall develop all training content, including course "leave behinds" such as summary sheets and reference material.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

The contractor shall document all planned training of FDIC personnel and submit plans to the FDIC for approval. The contractor shall cooperatively work with FDIC to modify submitted plans to accommodate FDIC needs for content, scheduling, and venues.

In addition, the contractor shall develop, administer, and maintain a self-paced Training Program (See **Section F, Deliverable 22**) for existing and new FDIC personnel that provide how-to instruction on specific, enterprise-wide support processes. Included in this training are service desk training for service desk customers, incident management system training for support personnel, and asset management for support personnel. See **Attachment MMM** for a description of what each of these trainings shall include at a minimum.

### **C.5.1.10     TECHNOLOGY INNOVATION**

The contractor shall facilitate an ongoing technology innovation process that identifies potential innovations and improvements to the FDIC environments, assesses the potential impacts, and is based on FDIC authorization and funding, executes the technological innovations. The contractor shall provide Technology White Papers and Briefings (See **Section F, Deliverable 23**) to the FDIC's management that provide the latest industry trends, and emerging technology and/or required technology refresh opportunities in the functional areas supported by this TO when requested and approved by the Oversight Manager. The contractor shall produce and document proposed recommendations for enhancements and improvements based on ITIL Level 3 practices. The contractor shall also provide technical experts as required for the effective implementation of new technology within FDIC.

The contractor shall provide the following information, at a minimum, when presenting a recommended technological action:

- a. Market awareness of technologies and IT capabilities that are applicable to FDIC's environment or as expressed to the contractor through governance processes.
- b. Predictions of market acceptance and adoption of technologies.
- c. Trends in computing and networking capabilities.
- d. Description of the issue/problem/opportunity
- e. Requirements analysis
- f. Functional and technical integration issues
- g. Recommended technical approach, its advantages and disadvantages, and how it will provide the most cost-effective solution
- h. Data and data sharing issues
- i. Security risks and risk mitigation measures
- j. Testing/benchmarking/implementation planning
- k. Estimated implementation costs/Lifecycle costs
- l. Rough Order of Magnitude (ROM) cost
- m. ROM schedule

### **C.5.1.11     TRANSITION SUPPORT**

Contract Number GS00Q09BGD0025  
Task Order GST0013AJ0084  
Modification PO12

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.1.11.1 TRANSITION-IN

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. Basic transition activities will be completed within the first 60 days, except as noted below. The contractor shall provide a Revised Transition-In Plan (**See Section F, Deliverable 24**), within ten workdays of completion of the kick-off meeting based on the contractor's proposal, that incorporates insights gained from being on site. The Transition-in plan should be updated regularly as the contractor gains additional knowledge of the FDIC environment. The contractor shall describe how the following, at a minimum, shall be performed during transition:

- a. Deliver all background investigation questionnaires, 7.5.2-1 (PGI) for all Key personnel to the FDIC OVERSIGHT MANAGER (**Section G. 3. 5.1**) within 2 business days of TOA (see Section H.7.1.1.1)
- b. Establish a prioritization and pre-screening of personnel for security clearances by the time of the TO kick-off meeting.
- c. Be prepared to process FDIC asset procurements by project kick-off.
- d. Fill all non-Key lead positions contained in **Section H.2.11** according to the described desired qualifications by the end of the transition period.
- e. Transition all maintenance and license agreements (**See Section J, Attachment DDD**) by the end of the transition period.
- f. Perform and deliver a draft Gap Analysis and Roadmap (**See Section F, Deliverable 40**) for bridging the gaps between the contractors approach and the current state of the FDIC IT systems and procedures by the end of the transition period.
- g. Transition all assets from the Fulcrum site not later than the end of the Base period.
- h. Perform a complete inventory of all assets not later than the end of the base period and reconcile the inventory with the AMS database and the latest inventory (note the differences between them). The contractor shall provide an Inventory Status/Reconciliation Report (**See Section F, Deliverable 25**) not later than the end of the base period.

After Government approval of the Transition-In Plan, the contractor shall perform in accordance with the Plan.

### C.5.1.11.2 TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan (**See Section F, Deliverable 26**) no later than 120 calendar days after commencement of final option period. The contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following, at a minimum:

- a. Project management processes

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- b. Points of contact
- c. Location of technical and project management documentation
- d. Status of ongoing technical initiatives
- e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
- f. Transition of Key Personnel
- g. Schedules and milestones
- h. Transfer of data, documentation, and processes
- i. Transfer of all maintenance and license agreements and ensure they are in compliance with the terms of **Section H.25** of the TOR.
- j. Actions required of the Government

The contractor shall establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings. The contractor shall provide an effective transfer of knowledge to effect a smooth transition.

### **C.5.2      TASK 2: ENABLING TECHNOLOGY SERVICES (ETS)**

The FDIC IT environment is a complex tapestry of technologies and capabilities, requiring attentive and proactive support. Support must be performed with a diligence aimed at ensuring the technologies are maximized and the capabilities are highly predictive in their availability and reliability. At its most basic level, all use of the FDIC IT infrastructure relies on the expertise and dedication of the infrastructure support team's technical approach and execution of service.

Enabling Technologies are defined as the infrastructure components that provide compute capability, data storage and manipulation, access and data transport, communications, and management control of all components. Each of these technologies is ever-evolving, with higher capacities and functionality being offered. FDIC approaches the adoption of evolved and new technologies with a cautious, structured, and well tested evaluation, seeking to embrace the appropriate changes at the opportune time.

The contractor's role in the Enabling Technologies area is threefold: (1) advise and consult, (2) operate, monitor, and maintain, and (3) control and manage. Under (1) advise and consult, the contractor shall act as a conduit of market and industry knowledge to FDIC, helping to increase the depth of knowledge and understanding of technologies as part of planning, architectural development, and standard usage. The contractor shall proactively seek opportunities to assist in the identification, evaluation, testing, and integration of new and emerging technologies. Additionally, the contractor shall contribute to the definition of technical architectures needed for the IT environment.

Under (2) operate, monitor, and maintain, the contractor shall perform the daily operational and managerial functions required to ensure continued performance of IT capabilities. This includes supporting all technology components. Contractor personnel shall not only be trained in necessary technologies and contractor products, they shall also have the experiential depth and

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

understanding of implementations being required under this TO to ensure optimal performance of the infrastructure.

Finally, under (3) control and manage, the contractor shall be the tactical arm of maintaining visibility into the performance of the IT infrastructure and exercising control over change. Through the use of FDIC-supplied infrastructure tools, the contractor shall monitor performance and capacity, feeding inputs that enable timely management decisions, on demand planning, asset expansion / replacement, and service to end users through the use of FDIC-supplied infrastructure tools. By controlling the introduction of planned changes, the contractor shall always be aware of the most common drivers of performance issues. Change control is crucial to maintaining normal operations.

The contractor shall perform these support roles on-site at FDIC Headquarters locations as necessary to physically manage the infrastructure and provide remote support to FDIC staffed non-FDIC Headquarters locations. As required, contractor personnel shall provide support services remotely, using network access to FDIC systems from established contractor delivery facilities. All contractor support and management actions shall be conducted in compliance with the FDIC established ITIL, COBIT, and FISMA design principals, as expressed and published by the Enterprise Management Services team in order to meet audit requirements. The contractor shall perform this work in accordance with the policies and procedures of EMS. Any exceptions to the process shall be documented and approved by FDIC. The contractor shall provide the following ETS support.

The contractor shall provide reports in support of ETS according to the specifications contained in **Section J, Attachment G**.

### **C.5.2.1     ENTERPRISE CONTROL PROCESS ALIGNMENT**

The contractor shall provide input, expertise, and advice on Enterprise Control Process development and enhancement to improve the FDIC IT leadership visibility into, control of, and management capability of the FDIC IT environment.

### **C.5.2.2     CROSS-TECHNOLOGY SERVICES**

The contractor shall comply with all strategy / infrastructure architecture / infrastructure standard requirements published by FDIC for use and deployment in the FDIC IT environment.

#### **C.5.2.2.1   DESIGN / DEVELOPMENT / VERIFICATION / PLANNING SUPPORT**

The contractor shall comply with all design / development / verification requirements published by FDIC for use and guidance in the FDIC IT environment.

- a. **Design Advisory:** The contractor shall provide input / consultation / advisory services to FDIC on systems design. The contractor shall strive to design any changes to the FDIC IT

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

environment (including operational changes) with a zero or minimal impact to the availability of systems, applications, or communications capabilities partly by identifying and recommending systems configurations to enhance redundancies and fail-over protections. Some of the input / consultation / advisory services may include the following activities:

1. When providing input to FDIC, include manufacturers' specifications and environmental requirements for appropriate system design, monitoring, and provisioning for devices installed on FDIC locations.
  2. Monitor and report on regulatory, legal, and political changes affecting the communications and computer industry at the Federal, state, and local level.
  3. Present proposals to FDIC for changes required to comply with regulatory, legal, and political changes so that FDIC may approve the changes.
  4. Review the compatible functionality among proposed software and device components and report on compatibility concerns to FDIC for adjustment.
- b. **Project and Task Management:** The contractor shall provide project and task support and management as part of meeting day-to-day requirements of delivery of services. Some of the project and task support management activities include, at a minimum, the following activities:
1. Comply with all project management requirements as assigned in the Enterprise Management Services specification and as periodically refined by FDIC.
  2. Work with FDIC project managers to define business, functional, and technical requirements and scope of projects.
  3. Prepare project proposals for FDIC internal socialization and project approval.
  4. Provide operational requirements for the scope of each project.
  5. Develop project plans to include a schedule and resource usage.
  6. Assist FDIC with cost / benefit justification for each project.
  7. Conduct project reviews in accordance with FDIC's requirements and methodologies.
  8. Provide oversight, coordination, and facilitation around acceptance of projects.
  9. Provide project management and technical expertise to optimize available resources.
  10. Monitor all contractor and third-party contractor tasks, coordinating with appropriate FDIC personnel.
- c. **Device or Software End-of-Life or Support:** The contractor shall inform FDIC Technical Monitors of device or software end-of-life or end-of-support events for devices and software deployed at FDIC. The contractor shall provide notification to FDIC within 10 business days of an end-of-life announcement by an OEM. The contractor shall provide a plan for the replacement of impacted device models within 120 business days of an end-of-life announcement, or identify and address them through the Technology Refresh Plan (See Section F, Deliverable 16).
- d. **Technical Refresh Plan (See Section F, Deliverable 16):** The contractor shall evaluate and report on FDIC's technology refreshment requirements and schedules for current devices,

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

technologies, and software no less than annually. The contractor may be directed to propose technology refresh projects based on FDIC-stated goals and substantiated in the contractor-provided technology roadmaps (see Enterprise Management Services) for Government consideration and approval. The contractor will maintain the deliverable and make updates as required or at a minimum, quarterly. In addition, prior to the submission of the quarterly deliverable, contractor will collaborate with the Government Oversight Manager and Technical Monitors to ensure that government required items are included within the Deliverable. The contractor shall identify and report on required upgrades to FDIC on a quarterly basis. Information shall include, but is not limited to, the following:

1. Devices/ software components required
2. Preliminary implementation plan to include resources
3. Total anticipated costs for investment and expenses
4. Impacted services and capabilities resulting by the proposed changes
5. Anticipated costs associated with acquisition of the necessary technology and supporting infrastructure
6. Anticipated timeline associated with commencement and conclusion of each refresh tactics
7. Identification of any pre-requisite refresh technology and associated project relationships
8. Identification of resource types and disciplines required to complete associated refresh projects
9. Anticipated value proposition and risks associated with completion of the refresh project or deferral as appropriate.

### **C.5.2.2.2 CHANGE CONTROL**

The contractor shall define and publish a change control process for use in designing, managing, and completing changes to the FDIC IT systems, networks, and capabilities. Additionally, the contractor shall comply with all change control process requirements published by FDIC IT. The contractor shall develop and propose a Maintenance Window Schema (**See Section F, Deliverable 27**) for all servers, mainframes, and network devices. For information on what the Maintenance Window Schema deliverable shall include at a minimum, see **Attachment NNN**. The contractor shall manage and maintain the maintenance window process. For a list of what the process shall include, but is not limited to, see **Attachment NNN**.

### **C.5.2.2.3 ENTERPRISE-WIDE COMMAND CENTER (EWCC) TO INCLUDE THE NOC**

The contractor shall provide an Enterprise-Wide Command Center (EWCC) for continual monitoring, measuring, oversight, troubleshooting, and management of FDIC telecommunications and computing capabilities, including the provisioning of situational awareness dashboards. If the contractor's proposal makes use of the Government's site, the Government will provide all utilities required for the continued normal operations of the systems, including electric power, uninterruptable power supply (UPS), and cooling. If the contractor is

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

providing support off-site, the contractor shall provide requisite work space for support personnel, including desks, telephony and network access.

- a. **EWCC Infrastructure:** The contractor shall perform, but shall not be limited to, the following activities:
  1. Evaluate and assess the current infrastructure that supports monitoring and perform gap analysis and make recommendations for improvements to current capabilities within 30 calendar days of the TO award.
  2. Support the development, implementation, and enforcement of physical security policies and procedures to ensure the protection of devices and to control access to FDIC systems and FDIC data.
  3. Develop a lifecycle management plan for all hardware and software under the purview of Enterprise monitoring.
- b. **EWCC Availability Monitoring and Incident Response Support:** The contractor shall provide 24x7 monitoring incident response for disruptions to all mission critical services hosted by the FDIC DIT. The contractor shall recognize, triage, investigate, and facilitate resolution of all Sev 1 incidents identified by the EWCC or transferred to the EWCC from the service desk.
- c. **EWCC Monitoring Toolset Integration:** The contractor shall integrate and make operational all FDIC-provided infrastructure monitoring tools for use by EWCC and the required workflow processes needed to conduct daily support activities. Such integration shall include, but is not limited to, providing the capability to monitor the health and status of Infrastructure components for all supported environments. The monitoring tools shall:
  1. Be capable of monitoring all devices and capabilities within the FDIC DIT Infrastructure environment to produce a clear understanding of component health and status, including but not limited to:
    - i. Network, data, voice, video
    - ii. Servers
    - iii. Storage systems and sub-systems
  2. Provide alerting and alarming events on occurrences in the IT environment.
  3. Allow the setting, adjusting, refining threshold values of usage or occurrences appropriate to the risk.Include a correlation engine component that collects data from all sources and deduplicates, translates, aggregates, decomposes and filters event information.
- d. **Toll-Free Contact:** The contractor shall provide the service desk a toll-free number for contacting the EWCC on a 7 day, 24 hour, 365 days a year basis.
- e. **EWCC Integration with FDIC:** The contractor shall provide integration services to facilitate the integration of EWCC monitors, alarms, and reporting with FDIC monitoring activities. Such integration services shall include, but are not limited to the following:



## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

1. Participation in integration planning and development meetings and planning sessions.
2. Cooperative development of interfaces and data exchange processes and tools.
3. Participation in testing of developed interfaces.

### C.5.2.2.4 INFRASTRUCTURE MANAGEMENT TOOLS

The contractor shall drive efficiencies in FDIC tool usage and make a recommendation for an efficient number of tools and the methods to properly implement those tools in an enterprise view.

- a. **Infrastructure Management Tooling:** The contractor shall develop the requirements for and provide an Infrastructure Management Tool (InMT) that is capable of managing all devices and capabilities with the FDIC environment. The InMT shall have, but is not limited to, the following functions:
  1. Management capabilities for accessing and controlling network devices, mainframe devices, servers, and associated peripherals.
  2. Application and
  - 3.
  4. Reporting capabilities of all the above.
- b. **InMT Data:** The contractor shall construct the InMT database and data storage such that all FDIC data shall be physically separated from access by non-FDIC personnel and non-FDIC support teams within the contractor organization. From the database, all InMT data shall have, but are not limited, to the following functions:
  1. Be readily available to FDIC for internal use.
  2. Be stored, managed, and protected in compliance with FDIC and governing policies.
  3. Be retained for the duration of 18 months.
  4. Be transferred to FDIC in a neutral or common file format prior to or at the end of the TO, upon request from FDIC.
  5. Be maintained in a format that is downloadable to Microsoft Excel / Access or a format FDIC designates.
- c. **InMT Access:** The contractor shall provide access to all InMT. This access shall be provided as follows:
  1. FDIC Technical Monitors and designated Subject Matter Experts shall have the ability to fully access the databases via the FDIC intranet, have the ability to actively use the tools for monitoring, investigations, troubleshooting, network management, performance tuning, and reporting by FDIC's command and control support time, have the ability to search real-time or near-real-time data (no older than four hours), and have the ability to perform ad hoc queries and report generation.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

2. Contractor access shall be provided to a maximum of 200 concurrent such users, with no more than 100, such named users.
  3. FDIC Technical Monitors and designated Subject Matter Experts shall have connectivity to the servers located at FDIC's premises and have administrator access (i.e., access to all menus and configuration, fault, and performance data) to these servers and storage sub-systems.
- d. **Device Management Data:** The contractor shall construct a database such that all FDIC data collected for device (e.g., network, server, storage devices) management shall be physically separated from access by non-FDIC personnel and non-FDIC support teams within the contractor organization. All data needs to be readily available to FDIC, be stored, managed, and protected in compliance with FDIC governing policies, and be maintained in a format that is downloadable to Microsoft Excel or Access or a format FDIC designates.
- e. **Real-Time Dashboard:** The contractor shall develop, implement, and maintain an Electronic Dashboard (See Section F, Deliverable 28) that provides real-time status of critical services and capabilities and key performance attributes of those services. Such a dashboard shall be constructed to perform and include the following, at a minimum:
1. Web based.
  2. Display FDIC selected performance data on FDIC services and capabilities.
  3. Multiple levels of controlled access according to the principles of least privileged.
  4. Provide current service status and performance data that is no older than 15 minutes.
  5. Support all licensed FDIC users with a minimum view access.
  6. Query primary sources of data whenever possible.
  7. Design and deployment should be consistent with FDIC DIT architecture standards.
  8. Ability to customize view for select customers.
  9. 98%Availability 24X7X365.
- f. **InMT Maintenance and Operations:** The contractor shall provide all required devices, software, databases, and other maintenance support required to maintain the InMTs. The contractor shall also configure and manage all operational, system management, and database support functions required to maintain the InMTs in working order.
- g. **InMT Utilization Monitoring:** The contractor shall monitor the use of each network segment and interface for throughput and each server and addressable storage sub-system on an FDIC-established and adjustable schedule with defined thresholds. The InMT shall trigger alarms at threshold levels and generate faults within the incident management system. For additional information on InMT utilization monitoring, see Attachment NNN.
- h. **Network Device Monitoring:** The contractor shall support advanced Fault Detection and Fault Isolation (FDFI) for all network devices. For additional information on Network Device Monitoring, see Attachment NNN.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- i. **Network Performance Data:** The contractor shall monitor all FDIC-defined network devices for selected performance values on an enterprise, segment, and individual link basis. The contractor shall provide statistics for the entire network by hour of day, business day, and the entire day. For a non-exhaustive list of statistics to actively collect and store, see **Attachment NNN**. In addition to those metrics listed in Attachment NNN, the InMT may collect other metrics required by FDIC to maintain a robust network operational situational awareness (e.g., event correlation, complex alerting, RCA capabilities), especially to include any new device or metrics without requiring a modification to contract. The InMT shall perform persistent quality tests of the environment to gauge response time, reporting on accuracy.
- j. **Server, Storage and Peripheral Monitoring:** The contractor shall implement, configure, and maintain tools to provide real-time, comprehensive monitoring of servers and supporting storage and peripheral sub-systems. Such monitoring shall collect and measure all data required to accurately generate required reporting and maintain supporting system responses (e.g., capacity planning, demand planning). For more information, see **Attachment NNN**.
- k. **InMT Reporting:** The contractor shall provide online access (preferably Web-based) to real-time and historical reports that can be downloaded. In addition, the InMT shall provide capabilities to generate standard report templates for key operational and situational awareness needs as well as ad-hoc reporting capabilities. For a list of minimum requirements for these reports, see **Attachment NNN**.
- l. **InMT Configuration Management Support:** The contractor shall configure and maintain the capability to access, and manage devices from a single tool executed in multiple locations. For a list of minimum requirements of support, see **Attachment NNN**.
- m. **InMT Configuration Database Management:** The InMT configuration database shall be updated as the environment is changed. (The InMT configuration database is the database that catalogs the inventory of all elements and devices and the configuration setting for those elements and devices). See **Attachment NNN** for a list of minimum requirements associated with the database management.

### C.5.2.2.5 TICKET AND INCIDENT HANDLING

The contractor shall comply with all of FDIC's IMS processes. The contractor shall be responsible for incident resolution and lead the coordination with all other contractors that are providing service to FDIC (e.g., LECs, carriers, software support contractors, and hardware service contractors). For information on the ticket and incident handling process, see **Attachment NNN**.

### C.5.2.2.6 BUSINESS CONTINUITY

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

The contractor shall develop, publish, and maintain Business Continuity Plans (See **Section F, Deliverable 29**) and steps, actions, and responsibilities for disaster recovery of all or portions of the FDIC IT capabilities. For information on disaster declaration, see **Attachment NNN**.

- a. **Annual Testing:** The contractor shall play an integral role and fully support FDIC in all planning and execution of semi-annual disaster recovery testing of the FDIC IT capabilities and services.

FDIC may conduct up to two disaster recovery tests per year. Such tests may be “desktop” tests or full-recovery tests and may include multiple portions of the FDIC IT environment and the devices and networks therein.

- b. **Essential or Critical Services:** If, at any time during the performance of this TO, the FDIC requires services essential or critical to its mission due to an actual or threatened emergency situation as declared by the Federal, state, or local authority, the contractor shall provide all resources necessary to support these services. The contractor shall be prepared to act immediately based on FDIC management direction if an actual or threatened emergency exists. The contractor shall take immediate and effective measures to ensure the availability or use of back-up or redundant services to support the emergency situation without any disruption. Any needed back-up or redundant services shall be provided for as long as the actual or threatened emergency situation exists.
- c. **Business Continuity Exercise:** The contractor shall support the annual Eagle Horizon Business Continuity Exercise each June.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.2.2.7 PATCH MANAGEMENT (ALL DEVICES)

The contractor shall perform comprehensive patch management for DIT- supported infrastructure. The contractor shall support the configuration and management of servers, networking, storage, and other peripherals, and facilities to support a test lab for patch evaluation. In addition, the contractor shall provide all system management and operational support of patch test systems and peripherals. The contractor shall use the approved tool set that support this environment.

- a. **Patch Identification:** The contractor shall implement a process for being notified of OEM patches released for each operating system (compute servers and sub-systems, mainframes, networking, telephony, and peripheral devices) and third-party software package installed on all devices. Software packages shall include applications, services, tools, communications software, and any other software approved by FDIC for execution on an FDIC device. Such a process shall ensure contractor is aware of new patches within two business days of release by the OEM.
- b. **Patch Deployment Verification:** The contractor shall develop, implement, and maintain a process to utilize the existing tool set to check each enterprise and personal computing platform monthly to validate the correct patch level is in place, to include documenting exceptions and mitigating risks. Independent verification should be done for all patched deployments to verify success deployment. Failed deployments shall be remediated.
- c. **Telephony - Patch Distribution – Scheduled:** The contractor shall design, engineer, implement, and manage a process and tool set to distribute patches to voice and VoIP devices. Each patch release shall meet the following requirements, at a minimum:
  - 1. Have been tested in a lab environment that mirrors FDIC voice and VoIP devices.
  - 2. Have been tested for interoperability with the un-patched elements of the voice and VoIP device.
  - 3. Have been approved by the OEM.
  - 4. Have been reviewed with FDIC and approved for release by FDIC.
- d. **Eligible Device Software and Databases for Support:** The contractor shall support device software and databases, within the requirements of the Services, for N-2 versions (where N equals the OEM's current major level release version) as part of the services.

Should FDIC determine the need to maintain any device at an OS or service version older than N-2 (where N equals the OEM's current major level release version), the contractor shall continue to provide support, but shall work with FDIC to determine the best balance of using an alternate pricing structure or relaxing service levels.

Any contractor-proposed alternative pricing model shall be accompanied by a clear, detailed cost analysis that clearly explains the proposed cost increase.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

In some instances, FDIC may be required by customer contracts to maintain databases at older versions. The contractor shall support these older versions as long as the OEM-determined, end-of-life date has not been reached. Support after the OEM end-of-life date shall be addressed through a best effort basis.

### **C.5.2.2.8 CABLE MANAGEMENT**

- a. **Cabling Engineering:** The contractor shall provide engineering support in the planning for new or modification to existing racking, cabling, and interconnections of equipment at the FDIC data center locations. For a non-exhaustive list of cable engineering support activities, see **Attachment NNN**. Support shall be for rooms housing servers, telephony, storage, and communications equipment.
- b. **Cable Management:** Following industry best practices and in coordination with responsible FDIC organizations, the contractor shall manage the installation and usability of cabling, racking, and interconnections at the specified locations. For additional information on cable management activities, see **Attachment NNN**.

### **C.5.2.3 SERVER SUPPORT SERVICES**

#### **C.5.2.3.1 SERVER INSTALLATION AND CONFIGURATION**

The Government will provide the following for FDIC-Maintained Locations in support of the servers, storage sub-systems, and peripherals located at FDIC locations:

- a. Provide all utilities required for the continued normal operations of the systems, including electric power, UPS, and cooling.
- b. Provide requisite work space for support personnel, including desks, telephony, network access, and common areas, such as restrooms, break areas, and conference rooms.
- c. Engineer, implement, and maintain environmental system to maintain normal operations as specified by device OEMs.
- d. Implement, and enforce security policies and procedures to ensure protection of devices and control access to FDIC systems and FDIC data.

The contractor shall provide device installation, configuration, de-installation, and preventive device management for servers, storage sub-systems, and peripherals. For information on the processes these activities, see **Attachment NNN**. In addition, the contractor shall monitor security for servers, storage sub-systems, and peripherals that are located at FDIC locations. See **Attachment NNN** for a list of non-exhaustive requirements for servers, storage sub-systems, and peripherals located both at FDIC locations and at the contractor facility.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.2.3.2 SERVER MANAGEMENT

The contractor shall provide leadership in identifying and evaluating new capabilities and technologies specific to the server environment. The contractor shall develop proposals for new technologies, capabilities, and processes. For a list of server management activities, see **Attachment NNN**.

- a. **System Software Installation:** The contractor shall install OS software on servers. For a list detailing the process for installing OS software on new servers, see **Attachment NNN**.
- b. **System Software Upgrades:** The contractor shall implement system software upgrades. For a non-exhaustive list of the processes involved in dot level or major level upgrades, See **Attachment NNN**.
- c. **Third-Party Software Installation:** The contractor shall install third-party software on servers. For a list of activities, see **Attachment NNN**.
- d. **Third-Party Software Upgrades (dot and major release levels):** The contractor shall install third-party software upgrades on servers. For a list of the types of activities associated with identifying and installing these upgrades, see **Attachment NNN**.
- e. **Virtual Server Instance Support:** The contractor shall support and maintain virtual server instances. A virtual server instance is a single operating system instance installed on virtualized physical servers. See **Attachment NNN** for a list of activities associated with this support.
- f. **Software Currency:** The contractor shall implement and manage a process to track the currency of all OS, database service, and other third-party software. For a list of non-exhaustive requirements associated with the currency tracking process, see **Attachment NNN**.
- g. **System Management and Monitoring Tools:** The contractor shall provide all equipment, OS software, network connecting equipment, layered software products, database software, probes, tooling software, tooling agents, and peripherals required to implement, activate, and sustain all monitoring and measuring requirements.
- h. **Server and Peripheral Device Monitoring:** The contractor shall implement, configure, and maintain tools to provide real-time, comprehensive monitoring of servers. Such monitoring shall collect and measure all data required to accurately generate required reporting and maintain supporting system responses (e.g., capacity planning, demand planning). See **Attachment NNN** for a non-exhaustive list of the requirements of the monitoring data.
- i. **Server Capacity Planning:** The contractor shall implement and maintain tools and processes necessary to provide capacity planning for the server environment. See **Attachment NNN** for a non-exhaustive list of these processes.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- j. **Server Performance Management:** The contractor shall implement and maintain performance management processes and tools for all servers. For a non-exhaustive list of the performance management requirements, see **Attachment NNN**.
- k. **Server Configuration Management:** The contractor shall implement and maintain the configuration management processes and tools for all servers. See **Attachment NNN** for a non-exhaustive list of the requirements associated with the configuration management process.
- l. **Backup Schema Planning and Implementation:** The contractor shall evaluate current backup and restore capabilities, technologies, and practices. For a list of the minimum requirements associated with backup schema planning and implementation, see **Attachment NNN**.
- m. **Media Management:** The contractor shall establish off-site storage requirements in accordance with FDIC's policies and procedures and document in the Operations Handbook. For a non-exhaustive list of additional requirements, see **Attachment NNN**.
- n. **Installs, Moves, Adds, Changes (IMAC):** The contractor shall perform all IMACs to the software and server device components and update the AMS with pertinent data regarding any such activity.
- o. **Incident Identification and Resolution:** The contractor shall identify deficiencies in the normal operations of servers, storage sub-systems, and peripherals and resolve all such issues:
  - 1. Where incidents are escalated from server operations, investigate and resolve the incident, and update service desk tickets with troubleshooting and resolution data.
  - 2. When required, engage other support teams, software developers, and device manufacturers.
- p. **Interfaces with FDIC Application Teams:** The contractor shall develop, foster, and maintain a close working relationship with FDIC service support teams. For more specific information, see **Attachment NNN**.

### C.5.2.3.3 SERVER OPERATIONS

The contractor shall provide 24x7x365 support for the servers implemented at FDIC. This includes maintaining high availability, incident response and remediation, and utilization reporting.



## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- a. **Operations Management:** The contractor shall provide day-to-day technical monitoring of the FDIC infrastructure. For a non-exhaustive activities associated with operations management, see **Attachment NNN**.
- b. **Console Operations:** The contractor shall operate server consoles in the course of normal server support functions and as part of troubleshooting and restoration activities.
- c. **Operations Handbook:** The contractor shall create an Operations Handbook (**See Section F, Deliverable 30**) for use by all contractor personnel providing server support services for FDIC servers, storage sub-systems, and associated peripherals. For a list of what the Operations Handbook shall include at a minimum, see **Attachment NNN**.
- d. **Command Procedures and Server Startup and Shutdown:** The contractor shall create, customize, and maintain startup and operational command procedures for all servers.
- e. **Administration:** The contractor shall perform administrative activities for all servers in accordance with FDIC policies and procedures including FDIC's security policies. These services shall be documented in the Operations Handbook. For a list of what these administrative activities shall include, at a minimum, see **Attachment NNN**.
- f. **Queue Administration and Management:** The contractor shall create batch and print queues at the request of the FDIC Technical Monitor. For a non-exhaustive list of activities associated with queue administration and management, see **Attachment NNN**.
- g. **Job Scheduling Tooling:** The contractor shall provide required tooling to enable job scheduling activities.
- h. **Daily Operations Documentation:** The contractor shall perform logging and reporting tasks associated with daily operations, including, but not limited to, the recording and auditing of fault reports, warnings, and alarms, and the implementation of call-out procedures for such warnings and alarms.
- i. **Monitoring:** The contractor shall actively and continuously scan, review, and respond to reported alarms, alerts, and notifications from established monitoring tools. For a list of what the monitoring activities shall include, at a minimum, see **Attachment NNN**.
- j. **Incident Acceptance and Resolution:** The contractor shall actively and continuously scan and monitor service desk queues established for the routing of server environment-related incidents. Accept and investigate tickets routed to such queues. See **Attachment NNN** for a list of what the contractor shall do, at a minimum, after investigating each incident:
- k. **Server Consumables:** The contractor shall monitor usage and order, and provide media (including magnetic tapes) consumables for the server environment.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.2.3.4 STORAGE MANAGEMENT

The contractor shall provide management of encryption keys for all encrypted storage. The contractor may also be required to repair defective devices, corrupted data, or software and then execute a full recovery of software and data on impacted drives by restoring a drive(s) using backup media. For the minimum requirements associated with key management, backup execution, and backup recovery see **Attachment NNN**.

- a. **Intrusion Detection:** The contractor shall execute the recovery of software or data using backup media when requested by an FDIC authorized user via the service desk or an FDIC service support team member by an established request process. For a non-comprehensive list of the requirements associated with intrusion detection, see **Attachment NNN**.
- b. **Media Management:** The contractor shall perform media management of FDIC media generated by backup processes from servers. For a list of what this process shall include, at a minimum, see **Attachment NNN**.
- c. **Media Management- Transportation:** The contractor shall establish a process and capability for off-site storage of FDIC media and the on-demand transportation of media to and from the location of the FDIC servers. For a list of the minimum activities associated with establishing this process, see **Attachment NNN**.
- d. **Media Management Equipment:** The contractor shall monitor media equipment for malfunction. See **Attachment NNN** for a list of these activities.

### C.5.2.3.5 EXTERNALLY FACING SERVERS

The contractor shall define enhanced security controls required for externally facing servers and encryption components.

- a. **System and Storage Sub-System Management Oversight:** The contractor shall provide all system and storage management and operational direction for externally facing servers and encryption components. See **Attachment NNN** for a non-exhaustive list of the oversight activities.
- b. **System and Storage Sub-System Onsite Support:** The contractor shall provide onsite support for externally facing servers and encryption components at the direction of the FDIC security teams. See **Attachment NNN** for a list of what this support shall include, at a minimum.

### C.5.2.4 SUPPORT OF THE SYSTEMS THAT SUPPORT THE DATABASE

The Government will develop, design, and perform build-out of FDIC-approved databases (e.g., Oracle, SQL, Informix, DB2 database technologies). The Government will execute the

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

databases on servers, security devices, mainframes, and other devices. The contractor shall establish a collaborative working arrangement with FDIC and FDIC-selected third-party application teams to encourage joint problem management and incident resolution activities. The contractor shall provide the following database administrative support, at a minimum:

- a. Monitor the databases on a frequent and regular basis to check for integrity, space utilization, and performance problems.
- b. Check on database logging systems including database lock errors and trouble shoot causes.
- c. Execute daily backups, review for success or failure, and restart within 60 minutes of any failures. All backups should be completed during off-peak hours of the day.

### **C.5.2.5    MIDDLEWARE SUPPORT - OPERATIONS**

The contractor shall provide the following middleware support, at a minimum (currently FDIC deployed products requiring support include Oracle products, Java, SQL, LDAP, DynaTrace, WebLogic, JVM, Datastage, Peoplesoft):

- a. Technical expertise in support of FDIC and FDIC named third-party development teams in scoping and planning for new application projects or modifications to existing applications. For a non-exhaustive list of how the contractor shall provide technical expertise, see **Attachment NNN**.
- b. Assist with the development and testing of new or revised applications. For a list of the activities the contractor shall perform at a minimum, **See Attachment NNN**.
- c. Maintain the capability to provide deep, technical support for all middleware products, technologies, and deployments with FDIC. Technical support shall be available 24x7 for Priority 1 incidents. For a non-comprehensive list of the on-demand support services that the contractor shall provide, see **Attachment NNN**.
- d. Participate in the development and execution of plans for the rollout of new or upgrading of existing application solutions that include the use of any middleware products. For a list of the minimum contractor participation requirements in the development and execution plans, see **Attachment NNN**.
- e. Maintain a cooperative working relationship with operations and services teams to enhance troubleshooting and support tasks.
- f. Provide Documentum engineering and operations support for an enterprise-wide environment. It is built on Redhat Linux and it leverages all components, including rights management, branch office, caching, records management, Bravia, in put Excel, and other components in support of a nationwide deployment for a mobile workforce. Legal, DOA, and RAD will make use of the capability.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- g. Provide Peoplesoft support for installation, implementation of products, batch processing, overseeing domains, administration, upgrades, deployments, and configuration on the Financial and Human Resources systems.

### **C.5.2.6 NETWORK SUPPORT SERVICES**

#### **C.5.2.6.1 NETWORK MANAGEMENT (EWCC NETWORK OPERATION CENTER (NOC))**

The contractor shall provide EWCC integration with existing FDIC IP address management tools for routine operational support needs and operational alerts. In addition, the contractor shall manage and maintain all of the WAN / Internet network devices for the full range of network services utilized by FDIC, utilizing the EWCC. See **Attachment NNN** for a minimum list of these services. The contractor shall manage and maintain all of the LAN / wireless/ voice / VoIP / teleconferencing network devices for the full range of network services utilized by FDIC; for a minimum list of these procedures, see **Attachment NNN**. In addition, the contractor shall perform the following activities.

- a. **Network Device Configuration Management:** The contractor shall perform the configuration management of network devices. See **Attachment NNN** for the minimum requirements associated with network device configuration management.
- b. **Capacity Planning and Forecasting:** The contractor shall perform capacity monitoring, reporting, and planning and have the capability to provide analysis and planning reports as requested. For a minimum list of the capacity planning and forecasting activities, see **Attachment NNN**.
- c. **Support for FDIC Headquarters and Non-FDIC Headquarters Locations:** The contractor shall perform on-site device management activities. See below for a list of the support the contractor shall provide, at a minimum:
  - 1. Device resets.
  - 2. Troubleshooting activities.
  - 3. IMACs.
  - 4. On-site support activities of encryption devices.
  - 5. Software and device upgrades and installations.
- d. **Onsite Device Support for FDIC Non-FDIC Headquarters Locations:** Provide on-site LAN management, network, and/or telecom support as needed.
- e. **Support for FDIC Personnel at Non-FDIC Headquarters Locations:** Provide remote support to FDIC personnel working at non-FDIC Headquarters FDIC locations. Support includes:

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

1. Troubleshooting and problem resolution.
  2. Guidance on configuration changes and management.
  3. Remote configuration changes.
- f. **WAN Administration:** The contractor shall perform WAN / Internet administrative and operational tasks including, but not limited to, the following:
1. Performing remote diagnostic and remedial maintenance procedures.
  2. Recommending configuration changes as appropriate.
  3. Monitoring usage of all consumables for the WAN environment (e.g., patch cables, cross connects, transceivers).
  4. Documenting operations procedures and services including procedures that affect operations.
- g. **LAN Wireless Administration for FDIC Headquarters Locations:** The contractor shall provide 24X7X365 Enterprise remote access support for the wireless services implemented at FDIC. This includes maintaining high service availability, incident response and remediation, and utilization reporting. The contractor shall perform LAN and wireless network administrative and operational tasks including, but not limited to, the following:
1. Performing remote diagnostic and remedial maintenance procedures when alerted to an incident by the triage function at the EWCC.
  2. Recommending and performing configuration changes as appropriate.
  3. Monitoring usage of all consumables for the LAN environment (e.g., Patch cables, cross connects, transceivers).
  4. Documenting operations procedures and services including procedures that affect operations.
  5. Performing and/or assisting with the static IP assignments in accordance with FDIC's approved procedure.
- h. **LAN Wireless Administration Support for FDIC Non-FDIC Headquarters Locations and Onsite LAN Support for FDIC Non FDIC Headquarters Locations:** The contractor shall provide 24X7X365 Enterprise remote access support for the wireless services implemented at FDIC. This includes maintaining high service availability, incident response and remediation, and utilization reporting. The contractor shall assist with onsite LAN management, network, and/or telecom support as needed. In addition, the contractor shall provide remote support to FDIC personnel supporting local LAN usage at non-FDIC Headquarters locations. Support shall include, but is not limited to, the following:
1. Troubleshooting and problem resolution.
  2. Guidance on configuration changes and management.
  3. Remote configuration changes.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- i. **Preventive Maintenance:** The contractor shall develop, implement, and maintain a Preventive Maintenance Program (**See Section F, Deliverable 31**), based on manufacturer guidelines and specifications, to include routine system, network, and device preventive maintenance to prevent, avoid, or reduce future service incidents. For a list of minimum routine preventive maintenance areas, see **Attachment NNN**.
- j. **WAN Configuration Database Updates:** The contractor shall update configuration database as the inventory is changed by any activity. For a list of what the updates shall include, at a minimum, see **Attachment NNN**.
- k. **LAN Configuration Database Updates:** The contractor shall update configuration database as the inventory is changed by any order activity. For procedures, see **Attachment NNN**.
- l. **Wireless Configuration Database Updates:** The contractor shall update configuration database as the inventory is changed by any order activity. For procedures, see **Attachment NNN**.
- m. **DNS / DHCP Management:** The contractor shall provide the following DNS / DHCP management support, at a minimum:
  - 1. **Provide DNS Services.** Services may include adding or removing zones, records, and hosts and configuring properties.
  - 2. **Provide DHCP Services.** Services may include adding networks, ranges, viewing and maintaining DHCP leases, and creating DHCP Network templates.
  - 3. **Provide IPAM Services.** Services may include and are not limited to:
    - i. Installing, relocating and re-installing, upgrading, and adding device or software components.
    - ii. Enabling or disabling services.
    - iii. Creating and maintaining read, read-write accounts with limited and/or full access.

### **C.5.2.6.2 IMAC SERVICES**

The Government is responsible for facilities readiness. The contractor shall provide IMAC services relevant to networks, zones, DHCP, etc. The contractor shall resolve outages and coordinate with the proper network carrier for network issues on behalf of FDIC. In addition, the contractor shall provide FDIC with direct access (e.g., live access or an outage bridge call) to its network engineering or other technical staff members. For additional procedures the contractor must adhere to, see **Attachment NNN**.

- a. **Network Capacity Monitoring, Reporting, and Planning:** The contractor shall perform capacity monitoring, reporting, and planning for all network services including WAN / Internet / wireless network services. For a list of minimum activities, see **Attachment NNN**.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- b. **Network Performance Monitoring, Reporting, and Develop Tuning Action Plans:** The contractor shall perform performance monitoring, reporting, and tuning for all network services. See **Attachment NNN** for a non-comprehensive list of activities and procedures.

### **C.5.2.6.3 REMOTE ACCESS & MOBILE CLIENT SUPPORT**

The contractor shall provide 24X7X365 Enterprise support for the remote access services implemented at FDIC. This includes maintaining high service availability, incident response and remediation, and utilization reporting. The contractors shall support connectivity to the network with Virtual Private Network (VPN) , SSL based web access , Citrix solutions, and Dial-in services, network optimization systems and authentication services. The contractor shall provide services support on a corporate-wide basis to include, but not limited to: support for bank examiner access; telecommuter access, and closing activities as determined by the FDIC.

- a. **Remote Access Support** - gateways and their associated systems are hosted at multiple FDIC sites. See **Attachment NNN** for a list of minimum activities the contractor shall perform.
- b. **Wi-Fi Network Support** – The FDIC deploys wireless (Wi-Fi) network solutions to support client access in FDIC offices and remote office locations. See **Attachment NNN** for a list of minimum activities the contractor shall provide/perform.
- c. **Closing Support** – Bank closing activities require that the FDIC deploy a secure network within each institution being closed. The Government is responsible for setting up the networks at the bank closing locations which are then connected to high speed internet services ordered and provisioned through various carriers by a team of FDIC-supplied contractors. The FDIC will determine the need for local network deployments to support bank closings. See **Attachment NNN** for a list of minimum activities the contractor shall perform.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.2.7 TELECOMMUNICATIONS PROVISIONING - BANK EXAMINER TELECOMMUNICATIONS SERVICES – BANK CLOSING SUPPORT

The contractor shall provide telecommunications provisioning and services support on a corporate-wide basis to also include support for Bank Examination Telephone Services (BETS) and closing activities as determined by the FDIC.

- a. **Telecommunications Provisioning** - The contractor shall coordinate and manage the installation, activation, ongoing support, and disconnect of both voice and data telecommunications facilities and their associated features/services on a corporate-wide basis. See **Attachment NNN** for a list of minimum activities the contractor shall perform.
- b. **BETS Support** - The FDIC routinely installs analog lines and, in some instances, high speed internet services in support of bank examination activities throughout the country. See **Attachment NNN** for a list of minimum activities the contractor shall perform.
- c. **Closing Support** – Bank closing activities require that the FDIC deploy a secure network within each institution being closed. Government personnel set up the networks at the bank closing locations which are then connected to high speed internet services ordered and provisioned through various carriers by a team of FDIC-supplied contractors. The FDIC will determine the need for service connections to support bank closings. See **Attachment NNN** for a list of minimum activities the contractor shall perform.

### C.5.2.8 TELEPHONY SUPPORT SERVICES

The contractor shall provide voice and VOIP system management support and administrative and operational activities. Contractor shall have staff available to provide telephony support from 6:00 AM until 10:00 PM Eastern Time. See **Attachment NNN** for a list of minimum activities associated with these activities. The contractor shall also perform preventive maintenance and develop, implement and maintain a preventive maintenance program. At a minimum, the preventive maintenance shall be based on manufacturer guidelines and specifications and should include routine system, network, and device preventive maintenance to prevent, avoid, or reduce future service incidents. Routine preventive maintenance areas may include the following:

1. System reboots.
  2. Capacity / utilization reporting.
  3. Tape backup rotation and off-site storage.
  4. Security updates to include password changes.
- a. **Configuration Database Updates:** The contractor shall update the configuration database as the inventory is changed by any order activity. In addition, the contractor shall provide



## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

detailed updates back to the FDIC triage function for completing incident documentation and ticket closure. For additional information, see **Attachment NNN**.

- b. **Device software support:** The contractor shall provide support for device software, within the requirements of the services, for N-2 versions (where N equals the OEM's current major level release version) as part of the services.
  - 1. Should FDIC determine the need to maintain any device at an OS or application version older than N-2 (where N equals the OEM's current major level release version), the contractor shall continue to provide support, but shall work with FDIC to determine the best balance of using a non-recurring initiative or relaxing service levels.
  - 2. Any contractor-proposed non-recurring initiative shall be accompanied by a clear, detailed cost analysis that clearly explains the proposed cost increase.
- c. **Perform Capacity and Performance Monitoring, Reporting, and Develop Tuning Action Plans:** The contractor shall perform capacity monitoring, reporting, and planning for all voice and VoIP services (See Attachment NNN for a list of minimum activities). The contractor shall also develop Tuning Action plans (See **Attachment NNN** for a list of minimum activities).
- d. **Voice and VoIP IMACs Support:** The contractor shall assist with facilities readiness for Voice and VoIP IMACs Support in accordance with asset and change management procedures See **Attachment NNN** for a list of minimum activities for each.
- e. **Voice Mailbox Management:** The contractor shall develop a process to integrate with FDIC Human Resources and facilities management teams at each site to handle notifications of requests for voice mailbox administration tasks. This process shall be presented to FDIC for review and approval. At a minimum, services shall include the following:
  - 1. Create new voice mailboxes.
  - 2. Delete voice mailboxes.
  - 3. Perform storage management.
- f. Perform administration and maintenance of the peripherals, i.e., Call Management System (Avaya IQ), Quality Monitoring (Witness), Integrated voice Response (Avaya IR), and Avaya Session Manager.

### **C.5.2.9 VIDEO / AUDIO CONFERENCING SUPPORT**

The Government will provide the facility and is responsible for facilities readiness. The contractor shall provide general conference support to include user and monitoring support provided from 6:00am – 10:00 pm Eastern Standard Time, facilities readiness, video conferencing device installation and configuration, capacity planning and management, and

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

technical assistance during video conferencing events. See **Attachment NNN** for a list of minimum activities.

### **C.5.2.10    MAINFRAME SUPPORT SERVICES**

The Government will provide the data centers for the mainframes. See **Section J, Attachment CC and Y** for an inventory of the mainframe hardware and software.

#### **C.5.2.10.1    MAINFRAME EQUIPMENT SUPPORT**

The contractor shall assist with selecting, contracting, and provisioning a maintenance and repair service for equipment to maintain normal operations. The contractor shall provide equipment maintenance support and mainframe equipment support. See **Attachment NNN** for a minimum list of procedures associated with these activities. The contractor shall be named as FDIC agent for invoking maintenance services.

#### **C.5.2.10.2    MAINFRAME SYSTEM MANAGEMENT SUPPORT**

The contractor shall analyze mainframe services and maintenance agreements for efficiencies. Responsibilities include, but are not limited to, the following activities.

- a. Provide problem resolution support.
- b. Provide support in accordance to the severity level assigned to incidents and problems.
- c. Provide contingency support.
- d. Work with other IT organizations as required.
- e. Carry out mass job control changes for programmers and authorized users.
- f. Provide technical support and administration for various data center products and service deployments.
- g. Provide system specifications to requesting authorized users or services groups in the pre-procurement stage of systems.

In addition, the contractor shall provide process and scripts to collect utilization data, develop capacity utilization models that compare current utilization to both physical capacity and logical capacity of mainframe sub-components. The contractor shall also monitor and validate capacity forecasts against FDIC's actual utilization and report monthly to FDIC on resource usage trends. Finally, the contractor shall develop and deliver Capacity Reports (**See Section F, Deliverable 70**).

- a. **Issue Identification and Resolution:** The contractor shall provide the following identification and resolution actions, at a minimum:
  1. Interface with the service desk to receive and accept tickets via the IMS.
  2. Populate tickets with troubleshooting and incident resolution data.
  3. Support troubleshooting activities with other support teams, both internal FDIC and third-party contractors.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- b. **Capacity Planning and Management:** Responsibilities with respect to capacity planning shall include the following activities, at a minimum:
1. Monitoring system use and capacity.
  2. Providing utilization reports to FDIC for its review.
  3. Providing capacity studies for systems considered for deployment in the environment.
  4. Forecasting a resource requirements plan.
  5. Providing space, CPU, and storage requirements according to FDIC forecasts.
  6. Analyzing and reporting resource trends.
  7. Analyzing service requirements.
  8. Monitoring and validating capacity forecasts against FDIC's actual utilization.
  9. Implementing, maintaining, and utilizing tools, techniques, and facilities for capturing and reporting relevant system utilization data.
  10. Communicating regularly regarding space availability, space-related abnormal ends (ABENDs), and areas of potential problems.
- c. **Performance Monitoring and Tuning:** The contractor shall provide the following performance monitoring and tuning support, at a minimum:
1. Conduct and report periodically as appropriate on systems performance reviews.
  2. Support FDIC's performance of service software, software, and equipment performance testing.
  3. Perform systems tuning in support of service software, software, and equipment operations.
  4. Monitor and improve overall performance of the systems environment through system tuning.
  5. Perform load balancing and other run time improvements.
  6. Install tools / products to improve the delivery of the services.
  7. Collect performance and utilization data for each CPU and storage device.
  8. Maintain a comprehensive performance database for the mainframe environment for 18 months.
  9. Review recent past performance trends on mainframe and midrange systems.
  10. Identify and correct processing slowdowns, malfunctions, and abnormalities.
  11. Provide monthly demand reporting to FDIC regarding CPU performance, utilization, and storage consumption.
  12. Perform regular monitoring of utilization needs and efficiencies.
  13. Report to FDIC on tuning initiatives monthly.
- d. **Software Tooling:** The contractor shall collect capacity and utilization data from mainframes and sub-components of mainframes, such as:
1. CPU
  2. Memory

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

3. Interfaces
  4. Storage sub-systems
  5. Network connections
- e. **FDIC Application Team Support:** The contractor shall support FDIC's application team. Support shall include, but shall not be limited to, the following:
1. Providing technical support, advice, and assistance as necessary to perform work on services software.
  2. Providing assistance related to product research, project support, and advice on service software tuning and efficiency improvements.
  3. Maintaining development and test environments for new software and service software releases.
  4. Maintaining quality assurance processes in accordance with FDIC infrastructure standard, or, if no FDIC infrastructure standard exists, industry infrastructure standards.
  5. Providing technical support and administration for products and service software roll-outs including analyzing service software resource requirements.

### C.5.2.10.3 MAINFRAME OPERATIONS SERVICES

The contractor shall take appropriate action to resolve mainframe-related problems. The contractor shall also respond promptly to requests from authorized FDIC personnel for priority job execution in accordance with FDIC-approved procedures. The contractor shall also provide spool and job control support (See **Attachment NNN**).

- a. **Command Procedures and Mainframe Startup and Shutdown:** The contractor shall provide the following command procedures and mainframe startup and shutdown support, at a minimum:
1. Create, customize, and maintain startup and operational command procedures for mainframe systems.
  2. Perform mainframe startups and shutdowns as required for normal operations, emergency situations, and recovery efforts.
- b. **Administration:** The contractor shall perform administrative activities (See Attachment NNN) for the mainframe equipment in accordance with FDIC policies and procedures relating to security.
- c. **Operational Tasks:** The contractor shall perform all console operations, including monitoring alarm systems and environmental controls, and transmitting and receiving information to and from outside organizations. For minimum operational processes and procedures, see **Attachment NNN**.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- d. **Job Schedule and Batch Queue Administration:** The contractor shall provide job schedule and batch queue administration support. See **Attachment NNN** for a list of minimum activities.
- e. **Implementing Change and Maintenance Window Execution:** The contractor shall provide implementation of change and maintenance window execution support. See **Attachment NNN** for a non-comprehensive list of procedures.

### C.5.2.10.4 DEPLOYMENT

The Government uses CA-Endevor for application code/processes and IBM System Modification Program/Extended (SMP/E) for the OS environment.

- a. **Planning:** The contractor shall coordinate installations, redeployment, and removal of equipment and software. The contractor shall also perform and coordinate any testing, scheduling, or systems integration of these items. For a list of minimum responsibilities with respect to deployment, see **Attachment NNN**.
- b. **Execution:** The contractor shall provide execution support. See **Attachment NNN** for a list of minimum requirements this support must include.
- c. **Issue Identification and Resolution:** The contractor shall provide issue identification and resolution support. See **Attachment NNN** for additional information.

### C.5.2.10.5 OUTPUT PROCESSING

The average monthly output volume is approximately 23,000 pages on the local printer and 28,000 to network attached printers. Output is electronically managed by Levi, Raye & Shoupe VTAM Printer Support (VPS). Output is archived using CA-View. The contractor shall perform the following types of output processing support:

- a. **Issue Identification and Resolution:** The contractor shall manage output on all output media in the mainframe computer environment. See **Attachment NNN** for minimum processes and procedures associated with this requirement.
- b. **Output Distribution – Electronic Output:** The contractor shall provide the following output distribution – electronic output support, at a minimum:
  - 1. Develop, implement, and maintain an electronic output process that delivers electronic output through the FDIC email system to authorized users based on an FDIC-defined recipient list.
  - 2. Update the recipient list when requested by the FDIC Technical Monitor.
  - 3. Provide such distribution in real-time, as output is generated.

### C.5.2.11 STORAGE SUPPORT SERVICES

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

The mainframe has a total of 38.4 Terabytes (TB) locally, half of which is used for business continuity volumes (BCV); of the remaining half, approximately 12.9 TB is usable storage, with 3.1 TB used by active data. All storage (including the BCVs) is replicated. The open systems environment has a total of 2.3 Petabytes (PB) of data, including storage located in the Virginia Square Data Center, Manassas Data Center, and Regional and Area Offices. The contractor shall provide storage management and operational support for all storage technologies deployed within the FDIC environment. In addition, the contractor shall perform storage management and support tasks for all activities. See **Attachment NNN** for a non-exhaustive list of tasks.

- a. **Server Data Management:** For both servers and mainframes, the contractor shall implement and administer a process for managing data life cycles. For information on what the process shall include at a minimum, see **Attachment NNN**.
- b. **Server Storage Operations:** The contractor shall perform storage operations activities for all servers. See **Attachment NNN** for a list of minimum storage operations activities.
- c. **Mainframe Storage Management:** The contractor shall perform storage management activities for the FDIC mainframe environment. For a non-comprehensive list of storage management activities, see **Attachment NNN**.
- d. **Mainframe Data Management:** The contractor shall implement and administer a process for managing data life cycles. See **Attachment NNN** for a list of minimum requirements.
- e. **Mainframe Storage Operations:** The contractor shall perform storage operations activities for the mainframe environment. For a list of minimum activities, see **Attachment NNN**.
- f. **Capacity Planning and Management:** The contractor shall perform capacity monitoring, reporting, and planning for the entire Storage & Backup environment. For a list of minimum activities, see **Attachment NNN**.
- g. **Backup Execution/Recovery:** The contractor shall provide backup executive support. When required to repair defective equipment or corrupted data or software, the contractor shall execute a full recovery of software and data on impacted drives by restoring a drive(s) using backup media to last fully recoverable backup, in accordance with industry best practices. As required, the contractor shall execute the recovery of software or data using backup media in accordance with FDIC business requirements and in alignment with industry best practices. For a minimum list of requirements associated with backup execution and recovery, see **Attachment NNN**.
- h. **Media Management:** The contractor shall perform media management of FDIC media generated by backups or data duplication processes from mainframes. For a list of what the media management shall include, at a minimum, see **Attachment NNN**. The contractor shall also establish a process and capability for off-site storage of FDIC media and the on-demand transportation of media to and from the location of the FDIC storage systems. For a non-

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

comprehensive list of offsite media management functions, see **Attachment NNN**. Finally, the contractor shall provide media management equipment support. See **Attachment NNN** for additional information.

- i. **Data Spills:** The contractor shall provide rapid and strict adherence to FDIC-approved policies and/or procedures for handling data spills. Data spills are data authorized to be accessible to a selected audience that has become available to unauthorized persons.

### **C.5.2.12 PRODUCTION CONTROL SERVICES**

The contractor shall provide schedule management support for all processing components (UNIX, Linux, mainframe, Windows Server, etc.) of the FDIC IT environment. The contractor shall also perform job schedule operations and perform issue identification and resolution tasks. See **Attachment NNN** for a list of minimum requirements that each of these activities must meet.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.3 TASK 3: CLIENT SUPPORT SERVICES (CSS)

As the entry point for interaction with service requests of the FDIC IT capabilities, client services demands a high level of attentiveness and ownership. Client services are comprised of the 11 service areas listed below. The role of the contractor in providing the Client Support Services (CSS) is to take ownership of service requests and manage those requests through end-user satisfaction based on the performance metrics contained in **(Section, J, Attachment D)**. The contractor may propose to establish the service desk and access control support functions at a contractor facility, leveraging teams and functionality in place. Support for FDIC end users located at any location other than FDIC Headquarters locations should be provided remotely whenever possible. Support requiring an on-site presence in non-headquarter locations will use on-site FDIC staff and on-site contractor staff in regional and satellite offices. Occasionally, contractor staff is dispatched to support non-FDIC Headquarters locations. Very rare (less 1% of all incidents) on-site contractor support is provided in the field sites. When support is required by field site staff they are handled through the closest regional office by having the equipment shipped to the regional site. All external communication with FDIC systems is provided with VPN or Citrix.

In this document, CSS are categorized and detailed in the following service sets. The contractor shall provide the support described in the following sections. The contractor shall provide reports according to the specifications contained in **Section J, Attachment G**.

- a. Enterprise Control Process Alignment
- b. Incident Management System (IMS)
- c. Service Desk Services
- d. Access Control Support (Identity Access Management System (IAMS))
- e. Desk-side Services
- f. Mobile User Support
- g. Wireless Device Support
- h. End-User Device Supports
- i. Printer Support
- j. Device Software Management
- k. IMACs – Installs, Moves, Adds, Changes

The following severity ratings are applicable to the types of incidents and the levels of incident management support:

“Severity” means the assignment of a value that indicates the importance and impact (realized or potential) of a problem. There are four severity levels.

“Severity 1” means mission critical – all incidents that require an immediate solution because FDIC cannot continue essential operations:

- mission critical or gold level application is down; or



## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- complete Production server or service failure (unavailability) that cannot be resolved by a restart or workaround; or
- degradation of a Production/Non-Production service/application impacting 10 or more users with the exception of Field Office network issues; or
- degradation of a Production/Non-Production service/application impacting that affects an application undergoing UAT in QA (list of affected servers compiled weekly based on UAT report from DMB).

Some examples are: email, global outage Prod/QA/DEV, WAN router outage in a Regional Office, NFE users complaining about extremely slow response, ETS Alert not functioning on workstations, production server indicated as being down in NetCool/Appboard, Regional Office bandwidth saturation alert over 90% for more than 15 minutes, and/or alert received in EWCC a building switch is down hard.

Non-production outages will be considered Sev-1 outages during normal duty hours, 7:00 AM to 7:00 PM Monday through Friday, not including Federal holidays.

“Severity 2” means high –

- incidents involving VIPs or a total outage at a Field office.

Automated ticketing system escalation pager/email notifications shall be sent in accordance with established escalation procedures. No more than ten percent of end users are designated as VIPs.

“Severity 3” means medium –

- incidents involving degradation or unavailability of a Production or Non-Production service/application known to affect fewer than 10 users, or
- Production or Non-Production server/service failure which has an established approved workaround or restart process to return service, or
- Critical application errors and network printer functionality otherwise interfering with essential business functions.

Examples include local DEV Zone down affecting a small group (< 10) of application developers (If not sure on numbers, default to critical severity), unexpected server reboots, disk space alert over 90% received in EWCC, or network printer outage or toner replacement.

“Severity 4” means low –

- incidents involving outages that affect single non-VIP user, or
- Incident has little impact on the FDIC community, or
- it is routine and has well understood resolutions or workarounds.

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

The following tier descriptions indicate the levels of support necessary to resolve an incident depending on its severity:

“Tier I” means initial support for basic client needs. The role of the contractor at this level is to gather customer information and make a determination of the customer issue by analyzing the symptoms and the underlying problem. Once the problem has been accurately identified and logged into the IMS, the contractor tries to resolve the client’s problem. Problems not resolved at this level are escalated to Tier II support. Tier I retains ownership of the problem. Each FDIC building has its own queue and its own FDIC Building Manager.

“Tier II” means a higher level of support than Tier I and is staffed by more experienced personnel that have a more in-depth knowledge about a particular product or service. Tier II problems may be handled remotely or in person. Tier II personnel assist Tier I personnel in solving technical problems or investigating elevated issues by confirming the validity of the problem and seeking known solutions to more complex problems or issues. If a problem is new and/or personnel cannot resolve it at this level, it is elevated to Tier III technical support.

“Tier III” indicates the highest level of technical support and this staff handles the most difficult and advanced problems. The contractor performs expert level troubleshooting and analysis of issues and problems. They are responsible for assisting Tier I and Tier II and for the research and development of solutions to new or unresolved issues. When a solution to the problem is determined, Tier III support is responsible for designing and developing one or more courses of action, evaluating each of these courses in a test case environment, and implementing the best solution to the problem. Once the solution has been verified, it is delivered to the client and made available for future troubleshooting and analysis. The problem or issue now becomes a known issue or problem and can be addressed at Tier I or Tier II support.

See the following attachment for historical ticket information:

**Section J, Attachment GG:** ISC Call Volume Data Sep 2011 – Feb 2012

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.3.1 ENTERPRISE CONTROL PROCESS ALIGNMENT

The contractor shall provide input, expertise, and advice on enterprise control process development and enhancement to improve the FDIC IT leadership visibility into, control of, and management capability of the FDIC IT environment. In addition, the contractor shall develop all IMS developments and implementations in compliance with FDIC established ITIL and COBIT framework, as expressed and published from the Enterprise Management Services team. Requests for exceptions to FDIC standard processes must be justified in writing with the reason for the exception and shall be approved in writing by FDIC.

### C.5.3.2 INCIDENT MANAGEMENT SYSTEM (IMS)

The software application Remedy is used to manage incident and problems tickets and to manage the routing of tickets between the contractors that support the ISC and ITAS contracts. The contractor shall interface with the ITAS contract through the use of the ISB-ISC Service Catalog (See **Section J, Attachment AA**), delivery council participation, and project meetings. The Government will provide all required OEM maintenance contract coverage for devices, software, and databases, required to maintain the IMS. The Government has space (See **Section H.5**) that is available for the contractor's solution. Its use is not required. The Government will provide an IMS to be used by the service desk to log, track, update, and manage incidents. The contractor shall configure all devices, software, processes, and procedures that are part of the IMS.

The contractor shall adhere to FDIC policies and procedures for incident logging and documenting incidents, participate in priority IRBs, and perform and support the RCA. The contractor shall document all incidents, including actions, investigations, and remediation efforts, in the IMS ticketing system implemented and maintained by the contractor at the service desk. The Government will provide the capability for FDIC-identified monitoring and alerting systems to automatically access the IMS and create a ticket in the IMS. The contractor shall configure the capability with guidance from the FDIC. The contractor shall develop, administer, update, and maintain all required workflows in the IMS. See **Attachment OOO** for a minimum list of these services. The contractor shall provide all operational, system management, and database support functions required to maintain the IMS in working order. For a list of how the contractor shall provide access to the IMS, see **Attachment OOO**. The contractor shall also provide the following.

- a. **IMS Configuration and Management:** As necessary, the contractor shall make and validate changes to the IMS system configuration and organization to maintain and enhance the IMS functionality. The contractor shall also create and maintain accounts for all users of the IMS, including contractor personnel, identified FDIC personnel, and third-party contractor personnel involved in the provision of services and approved by FDIC.
- b. **Incident Classification Process:** The contractor shall develop a Configuration Management Set of Classifications to be used in categorizing incidents logged into the IMS. The

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

contractor shall update the IMS as necessary to accommodate the defined classifications. The Government will participate in the creation of the classifications and may have up to 100 separate and distinct classifications.

- c. **Resolution Classification Process:** The contractor shall develop an Incident Resolution Set of Classifications to be used in categorizing the actions that result in an incident resolution. The contractor shall update the IMS as necessary to accommodate the defined resolution classifications. The Government will participate in the creation of the classifications and may have up to 200 separate and distinct classifications, with up to 20 sub-codes that categorize each action.
- d. **Non-ISC Ticket Queues:** The contractor shall develop a Ticket Queue Set of Classifications to be used in categorizing the actions that result in an incident resolution. The contractor shall update the IMS as necessary to accommodate the defined resolution classifications. The Government will participate in the creation of the classifications and may have up to 200 separate and distinct classifications, with up to 20 sub-codes that categorize each action.

### C.5.3.3 SERVICE DESK SERVICES

The contractor shall provide a 24x7x365 single point of contact (SPOC) service desk for end users to include, at a minimum, the following functionalities.

- a. Provide all support services in English.
- b. Provide a toll-free telephone function for use in calling the service desk.
- c. Provide a “quick-dial” function from FDIC telephony systems to reach the service desk using an abbreviated dialing number (currently \*999).
- d. Provide a chat capability where end-users may contact the service desk agents via chat or other FDIC-owned collaboration tool.
- e. Provide a 24x7x365 centralized service desk for all end users.
- f. Ability to provide the service desk and maintain the required level of service availability, including security, utilities, and protections, regardless if the offeror plans to have an on-site, off-site or blended service desk. If an off- site or blended service desk is proposed, FDIC may periodically visit the site for proper surveillance for performance.
- g. Staff the service desk with personnel trained in the technologies and products being supported and at the appropriate level for the support tier in which they are classified.
- h. Maintain a knowledgebase of solutions which can be accessed and utilized from both an IT technical support and end-user self-help perspective.
- i. Maintain a service desk staff that is professional in all interactions, trained to resolve issues, and focused on end-user and client satisfaction.
- j. Provide the capability to have a “broadcast” heard when accessing the service desk via the telephone and seen when accessing via the web. This broadcast shall announce known outages and issues, but may last for a maximum of 15 seconds on the telephone access.
- k. Voice messaging or other service for end-user to leave a message if overflow occurs due to concurrency capacity being reached.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- l. A customized greeting to all callers.

If the contractor provides this support offsite, he contractor shall provide an ACD for the routing, handling, and reporting of both inbound and outbound telephone calls to service desk that effectively interfaces with the FDIC internal ACD. The contractor shall also provide the telephony and connectivity for this support (e.g., all required telephony circuits, devices, software switching, and capabilities for telephony access) if this support is off site.

- a. Performing device remedial and preventive maintenance.
- b. Performing software installs, patching, and upgrades as required to ensure the ACD does not reach an end-of-life state from the OEM.
- c. Reviewing, designing, and implementing changes to the ACD as required to meet changing business needs.
- d. Review and design changes to the ACD as required to meet changing business needs.
- e. Providing design and implementation of ACD groups, call vectors, and enhanced call routing applications.

The Government will provide a tool used by the service desk to allow remote assistance via networking capabilities. The contractor shall implement, configure, and maintain the tool used by the service desk to allow remote assistance, via networking capabilities, for the purpose of remote diagnosis, troubleshooting, and repair of incidents. This tool will:

- a. Permit service desk personnel access to the end-user device and to view the screen at their location.
- b. Require a real-time, on-screen authorization from the end-user to permit service desk personnel to capture the device.
- c. Post a message on the end-user device when the remote capture connection has or will be ended.

See **Attachment 000** for a list of minimum processes and procedures the contractor shall follow if a telephone or chat-based service request is received; for service desk, web based, and automatic ticket logging; for automatic ticket logging and populating tickets; and for incident resolution, ticket updating, ticket dispatch, dispatch follow-up, dispatch coordination, ticket closure, ticket management, and time-stamping ticket activity. See below for additional service desk requirements.

- a. **Incident Severity Assignment:** Based on the severity definitions established for the services, the contractor shall assign a severity code to each ticket entered into the IMS. The severity shall be established based on, but not limited to, the following:
  1. A ticket logged by a named VIP or relating to a VIP device.
  2. An escalated severity as defined by a designated FDIC interface.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- b. **VIP Services:** For VIP or critical components, the contractor shall provide a Severity 1 level of troubleshooting and incident resolution. (See **Section J, Attachments EEE** for number of VIPs by location). Most Tier II VIP support is supplied by Federal staff in the FDIC Headquarters and in the fields/regions. Tier III infrastructure support shall be supplied by the contractor. Less than 1% of incidents are for VIP support. (See **Section J, Attachment GG** for call statistics.)
- c. **Consumer Off-the-Shelf Software (COTS) How-To Support:** The contractor shall provide “how-to” support to end users on corporate-wide COTS and limited-use COTS as needed by particular users. The contractor shall, at a minimum, provide the following support:
  - 1. Provide end users assistance in understanding how to use the features, commands, options, and uses of FDIC identified COTS software.
  - 2. Provide service for manufacturer’s current release of each software application, as well as support for up to N-2 (where N equals the OEM’s current major level release version) of the current version.
  - 3. Ensure service desk agents are appropriately trained in identified standard COTS to provide how-to support to novice application users.
  - 4. Provide services for the software applications detailed in **Section J, Attachment P**.
- d. **Ticket Age Escalation Process:** The contractor shall assist with developing an aging escalation process that identifies classes or types of tickets that will be escalated at specified ages for tickets routed to non-contractor resolution entities. The age escalation process shall provide a process for end users to escalate incidents that have not been closed in sufficient time or have been closed and were not resolved to the end user’s satisfaction. The age escalation process shall also provide the following, at a minimum:
  - 1. Detail the type and severity of tickets to be escalated.
  - 2. Detail all levels of an escalation hierarchy for each ticket type and severity.
  - 3. Detail the escalation ages for each ticket type and severity.
  - 4. Provide the escalation organization, IMS queue (if any), or contact name.
- e. **Resolution Coordination:** The contractor shall coordinate all incident resolution activities with all parties participating in the troubleshooting and resolution of an incident. As the coordinator, the contractor shall assume responsibility for the following, at a minimum:
  - 1. Ensuring all service desk, IMS, and resolution processes are followed.
  - 2. Providing a central point of communications for all troubleshooting and resolution activities.
  - 3. Instigating and maintaining communications with the end user, where appropriate, for scheduling dispatches, updating progress, and gathering data.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- f. **IMAC Scheduling and Coordination:** The contractor shall provide IMAC scheduling support for FDIC Headquarters and IMAC Coordination. See **Attachment 000** for minimum support the contractor shall provide.
- g. **Development and Use of Trending Data:** The contractor shall use the IMS data to proactively trend incident data and make environment change recommendations to FDIC to reduce and eliminate types and reoccurrence of incidents.
- h. **Service Desk Interfaces:** The contractor shall contact and co-resolve incidents with third-party contractors and/or FDIC support teams, when required. See **Attachment 000** for a non-exhaustive list of requirements associated with third-party contractors and/or FDIC support teams.
- i. **Scripting Interfaces:** The contractor shall develop, document, and maintain interfaces with FDIC application support teams, which shall include the following, at a minimum:
  - 1. Agreements with each separate FDIC group or team providing services.
  - 2. A template for documenting scripts to lead service desk personnel through a troubleshooting process for an FDIC-designated application.
  - 3. A process for feedback to the FDIC service teams on the effectiveness of the scripts provided.
- j. **FDIC Application Support Script Maintenance:** The contractor shall develop and publish to FDIC application support teams, an application support script maintenance Process and schedule for reviewing the currency.
- k. **The Contractor shall provide the following Bank Examiner helpdesk support:**
  - 1. Ticket creation
  - 2. Phone answering
  - 3. Determination of appropriate problem category
  - 4. Escalation to appropriate party(ies)
  - 5. Ticket closure
  - 6. Recordation of solution
  - 7. Creation/update knowledge library
  - 8. Password resets
  - 9. PDA assistance
  - 10. Remote connectivity access assistance
  - 11. Windows Office familiarity
  - 12. Single Point of contact for corporate users
  - 13. Insure input of 100% of reported errors/problems/issues
  - 14. “Ownership” of issue
  - 15. Develop and document help desk administration procedures
  - 16. Track, manage, and report help desk utilization

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

17. Provide escalation contact list
18. Issue broadcasts or other notices to provide status updates as required for planned and unplanned “events”
19. Develop and execute procedures for conducting end-user satisfaction surveys
20. Work with operational and technical staff to identify solutions that minimize the need to call the help desk
21. Receive and track requests for installations, moves, adds, and changes (IMACs)
22. Verify completion of IMACs by contacting the user to confirm satisfaction
23. Meet performance standards outlined in the service level metrics (See Section J, Attachment D)
24. Report and escalate security incidents as required in FDIC policy and procedures
25. Use Alert for password resets, correcting bank files, transferring files in and out of Alert, transferring files from Alert to Genesys, correcting database errors, fatal error messages, fixing functionality problems with the application. All scoping questions are sent to Wash-IS-DSC.
26. Use Genesys for password resets, fixing functionality problems, errors with pages, issues that involve transferring the files in and out. All database issues for Genesys are sent to Wash-IS-DSC
27. Use FDICconnect to deal with all issues regarding FDICconnect. The contractor will not directly assist with several of the transactions, e.g. is the Assessment Statements transaction for which the contractor helps grant access and refers everyone with questions regarding the statements to the Assessment payment hotline.
28. Using Vision for Password resets, IAMS request, known errors. For errors involving the SAER page the client is referred to Vision Support.
29. Handle issues involving CCA, CDL, Exam Transmittal, IER, IRRSA, SCOR, Sharp, Source, STARS, and Pro. These are generally sent to Wash-IS-DSC for resolution unless there is a fix sent from development team detailing how to resolve the issue.
30. Receive calls involving Extranet and insurance coverage that get transferred to Entrust and the Call Center respectively.

### **C.5.3.4 ACCESS CONTROL AND IDENTITY MANAGEMENT (IDM) SUPPORT**

As part of the Access Control Support, the Government will provide the devices, software, facilities, on-going physical environment, and security controls and access capabilities to an Identity Access Management System (IAMS) to provide controlled access to FDIC systems, devices, and networks. The Government will provide process requirements for evaluating, approving, and granting access via the IAMS tool. The access control front end (ACFE) function is a client-facing service responsible for ensuring all access requests are being processed through the IDM system, IAMS. To accomplish this goal, the ACFE function work closely with IAMS Administrators, Helpdesk and Security teams to ensure that proper FDIC Information Security policies are followed. The IDM administration is responsible for the operation of the IDM system and all the connection points such as AD, Mainframe, Remedy, reporting datamart, etc. The contractor shall provide request management support, IDM operational support, IDM



## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

testing and administration tasking. See **Section J, Attachment OOO** for minimum tasking and support requirements.

### **C.5.3.5**                      **DESK-SIDE SERVICES**

Desk-side support is key to providing FDIC users with high quality service. The contractor shall supply Tier II desk-side support at FDIC locations throughout the U.S. based on Government-supplied service level metrics (**See Section J, Attachment D**). Support for regional and temporary satellite offices shall be supplied by both permanent onsite presence and by dispatching contractor personnel. Dispatching of contractor personnel to field sites is very rare and must have prior approval from FDIC before any dispatch can occur. When Government staff is having an issue with a device they take it to the nearest regional office for a decision on fixing or replacing the item. The Government or contractor may call a third-party contractor to repair/replace the item. See **Section J, Attachment F** for the service locations.

- a. **Device Preventive Maintenance:** The contractor shall perform preventive maintenance activities for end-user devices when required. For a non-exhaustive list of preventive maintenance activities, see **Attachment OOO**. The contractor shall also perform device and software remedial maintenance when required in accordance with FDIC procedures.
- b. **Training Room Setups:** The contractor shall, when requested via a service desk ticket, complete the necessary setup of training rooms at the FDIC Headquarters locations. Historically setup has included:
  - 1. Installation of devices (e.g., PCs, LAN equipment, printers).
  - 2. Setup and configuration of devices.
  - 3. Testing to ensure normal operations of the devices.
  - 4. Work with on-site facility and training personnel in finalizing the room for use and support it during use.

### **C.5.3.6**                      **MOBILE USER SUPPORT**

The contractor shall provide access to service desk capabilities and tooling to end-users who are located remotely from an FDIC location. In addition, the contractor shall provide a process to replace devices that, at a minimum, includes:

- a. Distribution to all traveling and remote end-users of overnight shipping envelopes with pre-printed ship-to addresses and expense codes.
- b. Maintenance of an inventory of spare devices for configuring and same-day shipping to end-users.
- c. The capability to recover backed-up data onto spares and / or repaired machines from a remote location.
- d. The repair and return of the end-user device to the end user after repair work is complete.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.3.7 **MOBILE DEVICE SUPPORT**

The contractor shall provide all software update, patching activities, and device maintenance activities required to maintain normal operations of mobile client devices. In addition, the contractor shall maintain support relationships with mobile device OEMs to have access to OEM support teams and engineering functions.

### C.5.3.8 **END-USER DEVICE SUPPORT**

The FDIC uses single Standard Operating Environment (SOE) images that are modified for each type of user (See **Section J, Attachment BB** for the Base Image). The contractor shall provide the following end-user device support, at a minimum.

- a. **System Software Support Services:** Provide all software update and patching activities required to maintain normal operations of end-user devices. Additionally, the contractor shall maintain support relationships with systems software OEMs to have access to OEM support teams and engineering functions.
- b. **Device Support Service:** Either remotely or on-site, triage hardware failure incidents and:
  1. Determine most likely reason for failure to maintain normal operations.
  2. Verify warranty coverage or maintenance coverage for device.
  3. Using an established work flow process via the service desk, engage repair services to resolve the incident and return the device to normal operations.
  4. If appropriate, update the AMS.
- c. **Reimaging:** To resolve an issue, with an end-user device, the contractor may be required to reimage the device in accordance with procedures.
- d. **Event Support:** Provide onsite support for end-user devices during major events such as conferences and leadership meetings.

### C.5.3.9 **PRINTER SUPPORT**

The contractor shall provide the following printer support, at a minimum in accordance with FDIC procedures:

- a. Printer Installation, configuration, and testing
- b. Preventive maintenance
- c. Maintenance and repair
- d. MACs
- e. Inventory management

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

### **C.5.3.10 DEVICE SOFTWARE MANAGEMENT**

The contractor may be required to perform manual installation of software, manual modifications to software, or the manual de-install of software on a device. The contractor shall also support OS software and service software, within the requirements of the services, for N-2 versions (where N equals the OEMs current major level release version) as part of the services.

### **C.5.3.11 IMACS – INSTALLS, MOVES, ADDS & CHANGES**

The contractor shall co-plan all staging and deployment of new devices with the Engineering and On-Demand (EOD) services team. Such cooperative planning shall include, but is not limited to, the following:

- a. Participate in planning activities.
- b. Assist EOD team in the final validation of functionality of new devices.
- c. Align deployment plans with other priorities in the end-user environment.
- d. Validate deployment processes for thoroughness and accuracy.

For a non-exhaustive list of processes and procedures involved for IMACS, see **Attachment 000**. The contractor shall also develop an IMAC Expedite Process to expedite IMAC requests beyond the performance levels provided in the performance metrics (**See Section J, Attachment D**).

### **C.5.4 TASK 4: PROTECTION AND ASSURANCE SERVICES (PAS)**

FDIC is keenly aware of the importance of computer security since it is an organization tightly coupled with U.S. Government and U.S. financial organizations. It is critical to the operation and reputation of the FDIC that only authorized persons are able to access FDIC systems, networks, and data. For this reason, it is crucial that all IT support functions, from application design to PC login processes, are designed, built, and managed in alignment with security requirements.

There are multiple sources of security requirements and demands for the FDIC IT environment. U.S. Government agencies, FDIC directives, and other governing bodies continuously identify vulnerabilities and develop protection policies and tools to thwart attacks and maintain appropriate security. The FDIC IT organization must remain vigilant in its awareness of threats, and be prompt and thorough in addressing identified risks. The Protection and Assurance Services (PAS) described within this task are designed to define the requirements that shall ensure FDIC achieves a high level of attention and response to security issues.

The contractor shall have a substantial role in successfully implementing the PAS service. The Government will retain oversight of all security actions and policies. The contractor shall support the security function as an industry expert in technologies and security practices, proposing and enhancing FDIC's security implementations.

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

The PAS services are categorized and detailed in the following service sets.

- a. Enterprise Control Process Alignment
- b. Policy and Procedure
- c. Security Operations Support
- d. Prevention and Recognition

All security developments and implementations shall be developed in compliance with adherence to ITIL, FISMA, and COBIT framework. Any exceptions to the process shall be approved by FDIC and documented as to reasoning.

Historically, the Government has required the development of approximately six contractor-created security policies and procedures per year. The Government has also required the update of approximately ten procedures per year.

The contractor shall provide reports in support of PAS according to the specifications contained in **Section J, Attachment G**.

### **C.5.4.1 ENTERPRISE CONTROL PROCESS ALIGNMENT**

The contractor shall provide input, expertise, and advice on enterprise control process development and enhancement in order to improve the FDIC IT leadership understanding of the FDIC IT environment. To ensure continued alignment with enterprise control processes and maintenance of a security focus in the delivery of all services, the contractor shall ensure its operations and service delivery processes are compliant with FDIC's Security Requirements (e.g., FISMA, NIST), policies, and procedures related to security. The contractor shall also facilitate the development of standard operating procedures for operational security functions.

### **C.5.4.2 POLICY AND PROCEDURE**

The Government is responsible for developing and publishing policies related to security processes and controls to be implemented in the FDIC IT environment. The contractor shall also develop procedures to show how the contractor is maintaining compliance. The procedures shall:

- a. Comply with all appropriate FDIC security directives and related Government regulations and legislation.
- b. Detail actions and requirements for all personnel involved in the use and support of FDIC IT infrastructure components and capabilities.
- c. Be developed in alignment with published FDIC policies and directives.
- d. Be published in a manner consistent with FDIC policies.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

The contractor shall also update security procedures for currency and applicability in a manner to reflect changes in requirements as detailed in FDIC directives and Government regulations and legislation. These maintenance processes shall include, but is not limited to, the following.

- a. Scheduled reviews of procedures.
- b. Ad hoc reviews based on new requirements and new technology capabilities.
- c. Emergency reviews to address security incidents and identified vulnerabilities.

The contractor shall ensure that all contractor personnel and support actions are in alignment with policies and procedures governing FDIC, including Office of Management and Budget (OMB) policies, NIST regulations, FISMA, Federal Information Processing Standards (FIPS), Common Criteria, and FDIC directives. These policies and procedures shall evolve over the period of performance. Compliance shall evolve in step with changing requirements and new requirements that may be approved by FDIC.

### C.5.4.3 SECURITY OPERATIONS SUPPORT

- a. **Operations and Maintenance Support for Security Devices:** The contractor shall perform the following operations and maintenance tasks for security-managed devices. This service includes, but is not limited to, the following.
  - 1. URL and application access requests.
  - 2. Custom rule access requests.
  - 3. Firewall port change requests.
  - 4. Secure-email TLS configuration requests with external organizations.
  - 5. VPN tunnel establishment and monitoring.
  - 6. Email/spam/phishing messages investigation support.
  - 7. Full system/application integration services into the FDIC perimeter security architecture.
  - 8. Configuration change workflow generation, maintenance, and documentation.
  - 9. Access and Authorization workflow generation, maintenance, and implementation.
  - 10. Participate in integration and transition activities for engineering solutions.
  - 11. For a list of the minimum devices/technologies, see **Attachment PPP**.
- b. **Application Security Appliances:** The contractor shall support application security devices by evaluating, implementing, upgrading, and maintaining said devices. The contractor shall also work with developers to ensure code changes and additional sites and applications are protected by the application security device and that the site is accessible. The contractor shall implement changes in development, quality, and production. This support is provided in cooperation with Task 6.
- c. **Endpoint Security Support:** The contractor shall provide overall operational support for all endpoint services for security applications. For a non-exhaustive list of what this support shall include, see **Attachment PPP**.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- d. **Antivirus Support:** The contractor shall install, maintain, and monitor antivirus products and processes on end-user devices and servers. For a list of what this service shall include, at a minimum, see **Attachment PPP**.
- e. **Application Whitelisting Support:** The contractor shall install, maintain, administer, and execute application whitelisting endpoints. For a list of what this service shall include, at a minimum, see **Attachment PPP**.
- f. **Host Intrusion Prevention Support (HIPS):** The contractor shall install, maintain, administer, and execute host intrusion prevention software and tooling. For a list of what this service shall include, at a minimum, see **Attachment PPP**.
- g. **Public Key Infrastructure (PKI) and Extranet and Backend Support:** The contractor shall provide support of the PKI infrastructure and extranet and its associated components. For a non-exhaustive list of activities involved in this support, see **Attachment OOO**. In addition, the contractor shall provide support to the PKI engineering efforts. For a list of what this support shall include, at a minimum, see **Attachment PPP**.
- h. **Back-End Access Control Support:** The contractor shall provide support for the back-end access control processes, tools, software and hardware to include Tier 1 and 2 support to resolve entrust and extranet issues and Tier III when required for advance PKI issues. For a non-exhaustive list of what this support shall include, see **Attachment PPP**.
- i. **Access Control Facility (ACF2) Support:** The contractor shall provide technical and analytical guidance on security control issues for the mainframe, to include Tier III support when required. For a list of activities, see **Attachment PPP**.

### C.5.4.4 PREVENTION AND RECOGNITION

- b. **Security Monitoring Reports Distribution (SECMRD) Support:** The contractor shall assist with developing and publishing architecture and requirements for SECMRD system structure, outputs, and functionality. The contractor shall also design and implement any major enhancements to the SECMRD. These enhancements include, but are not limited to, the following:
  - 1. New API development, test, and implementation.
  - 2. OS-schema and directories extraction.
  - 3. Batch job development.
  - 4. Database structural changes.
- c. **SECMRD Operations:** The contractor shall maintain SECMRD system operations (that support ISM and IT resource-owners). For a list of what this requires, at a minimum, see **Attachment PPP**.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- d. **SECMRD Monitoring:** The contractor shall design, test, implement, and maintain a monitor-based solution under FDIC guidance and SECMRD requirements. For a list of what this service shall include, but is not limited to, see **Attachment PPP**.
- e. **SECMRD Reporting:** The contractor shall collect and review SECMRD reports for anomalies and issue identification. For a list of what this service shall include, at a minimum, see **Attachment PPP**.

### C.5.5 **TASK 5: ENGINEERING AND ON-DEMAND SERVICES (EODS)**

The FDIC IT environment is a complex configuration of technologies that must interact reliably to support the FDIC's business operations. The ebb and flow of new and emerging technologies drives a constant demand to engineer new solutions, improve existing deployments, and ensure all environmental components are operationally integrated. Spanning all aspects of the capabilities of FDIC IT as described in ETS (**See Section C.5.2**), and infrastructure architecture & standards planning as described in EMS (**See Section C.5.1**), engineering services must be attentive to detail, technically deep in ability, and broad in its understanding of FDIC IT to lead the strategic planning and tactical execution of enterprise services to facilitate FDIC business goals.

There are three principal elements to the engineering services: (1) Project Planning and Support, (2) Technology, Engineering, and Tier III Support, and (3) On-Demand Services. Project planning is crucial to ensuring desired technology implementations are well thought out and thoroughly planned. This includes ensuring preparedness for the technical aspects of a project and predicting resource needs and costs associated with the project. Rigorous planning increases the probability that projects shall be successful, on time, and within budget.

Project support requires attention to the goals of the project outcomes and the project management needs of FDIC. All projects must be staffed by competent and knowledgeable staff members who are well versed in both the technologies being deployed and the intricacies of the FDIC IT environment. Project management oversight must be embraced by the contractor. Additionally, the contractor shall adhere to FDIC Engineering policies, procedures, and reporting processes. See **Section J, Attachment CCC** for a list of projects and their current status.

Technology and Engineering support requires researching, planning, designing, architecting, implementing new technologies as well as upgrading, maintaining, and supporting existing infrastructure technology systems. Tier III support requires to provide expert advice, troubleshooting, and supporting existing systems.

On-demand services provided a vehicle for assisting FDIC staff with specific technology needs. Resources with specific expertise may be needed for evaluations, special projects, or short or long term ancillary support of IT capabilities.

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

In addition to all engineering solutions described in ETS, image, patch, service pack, and upgrade support requirements call for a disciplined approach to the creation and maintenance of standard images for end-user devices, servers, and other devices. Two key elements of this service are the strict adherence to quality testing and management of a process and integration to the existing systems to ensure timely distribution of new images. Service packs, upgrades, and patch management is crucial to the success of organization. As an organization serving the public trust and housing sensitive information regarding the U.S. financial market, the ability to rapidly react to a security threat as well as functionality upgrades through patch evaluation and distribution, service packs, and upgrades. FDIC must have a responsive, attentive approach to identifying and implementing patches, service packs and product upgrades. This requires cooperative interaction with security and various infrastructure support teams. The contractor shall assume responsibility for image, patches, service packs, and product upgrade support activities. This includes leveraging experience in patch identification and evaluation to the benefit of FDIC.

Project support resources shall be a combination of FDIC and contractor personnel, with exact roles, quantities, and skills determined on a project-by-project basis. The contractor shall provide varying levels of management of these projects. The contractor shall rapidly provide on-demand services and integrate into Government/contractor teams to provide engineering solutions as they are needed.

It is important to note that services provided as part of EODS shall span the breadth of technologies and IT capabilities at FDIC. Servers, OS, networking, personal computing, middleware, storage, mainframes, and anything on the horizon shall be candidates for support, and FDIC will rely on the contractor to provide trained and experienced personnel to meet the on-going need.

In this document, EODS are categorized and detailed in the following service sets.

- a. Enterprise Control Processes
- b. Engineering Project Services
- c. Technology Refresh and Software Maintenance
- d. On-Demand IT Services
- e. TIER III Support Services
- f. Image Engineering
- g. Patch Management, service packs, and product upgrades



## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### **C.5.5.1     ENTERPRISE CONTROL PROCESSES**

The contractor shall provide input, expertise, and advice on enterprise control process development and enhancement. All engineering developments and implementations shall be developed in compliance with FDIC established ITIL and COBIT and FISMA design principles. All engineering developments and implementations shall also be developed in compliance with FDIC-established security policies and requirements, as expressed and published from the enterprise management services team and IT security leads.

The contractor shall develop, propose, manage, and complete all engineering development and implementation projects as defined in a project plan. All project plans shall be developed and managed in compliance with the project management requirements detailed in EMS and FDIC DIT Project Development Life Cycle processes. For projects that are assigned to the contractor, the contractor shall maintain the milestones and results of the Government-approved project plans. This will be the basis of the Government's performance-based monitoring for this task area. For projects led by FDIC, the contractor shall provide timely inputs, updates, and assistance in developing project plan report outs.

### **C.5.5.2     ENGINEERING PROJECT SERVICES**

The contractor shall identify necessary deployments, improvements, or changes that will enhance the overall performance or address a specific service issues within the FDIC IT environment. For a list of where this identification may originate, see **Attachment QQQ**. The Government will also identify project needs. For a list of where this identification may originate, see **Attachment QQQ**. For a list of project support activities the contractor shall perform, but is not limited to, see **Attachment QQQ**.

The contractor shall develop a Preliminary Project Plan (**See Section F, Deliverable 32**) based on defined project goals and expected outcomes. For a list of what this plan shall include, see **Attachment QQQ**. Once approved by the Government, the contractor shall maintain the project plan and provide updates as required.

### **C.5.5.3     TECHNOLOGY REFRESH AND SOFTWARE MAINTENANCE**

The contractor shall provide the following types of engineering support in planning and implementing new technologies with surge requirements.

#### **C.5.5.3.1   TECHNOLOGY REFRESH**

The contractor shall provide resources to support FDIC in engineering and project management of hardware and software refresh projects as part of FDIC standards and the emerging technology refresh cycle. The contractor shall perform, but is not limited to, the following.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- a. Evaluate FDIC’s technology refreshment requirements and schedules for current devices, technologies, and software no less than annually.
- b. Propose technology refresh projects based on FDIC-stated goals and substantiated in the contractor-provided technology roadmaps.
- c. Identify and report on required upgrades to FDIC by May 15 of each year and quarterly thereafter, including but not limited to the following,
  1. Devices / software components required.
  2. Preliminary implementation plan.
  3. Total anticipated costs for investments and expenses.
  4. Impacted services and capabilities resulting by the proposed changes.

### **C.5.5.3.2 SOFTWARE MAINTENANCE**

The contractor shall provide software currency information, software maintenance, software support, and software release management. See **Attachment QQQ** for a list of the minimum support the contractor shall provide. The contractor shall comply with enterprise-wide control processes under Enterprise Management Services (Task 1) and shall be tightly integrated with the services provided with Development, Quality Assurance, and Testing System Support task area (Task 6).

### **C.5.5.4 ON-DEMAND IT SERVICES**

When requested by FDIC, the contractor shall address specific information technology needs within the FDIC IT environment. The required on-demand services may include planning, engineering, implementation, and knowledge transfers for new technology with specific subject matter expertise in the following types of areas:

- a. FDIC deployed network, server, or storage operating systems (e.g., Unix, Wintel)
- b. Storage technologies
- c. Server technologies
- d. Network technologies
- e. Database technologies
- f. Wireless technologies
- g. Messaging and collaboration technologies
- h. Middleware technologies
- i. Asset management technologies
- j. Voice and video technologies
- k. Remote access technologies
- l. Web server services and technology
- m. Emerging technologies
- n. End-user productivity technologies

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.5.5 TIER III SUPPORT SERVICES

The contractor shall provide Technology Tier III support services to FDIC end users, FDIC support teams, and contractor support teams. In addition, the contractor shall design activities within the FDIC IT environment. For a list of services that the contractor shall perform, but is not limited to, for Tier III support and design, see **Attachment QQQ**. The contractor shall also maintain the capability to provide deep technical support for all middleware products, technologies, and deployments with FDIC. Support shall be available 24x7x365 for Priority I incidents. For a list of minimum requirements involved in Middleware Tier III support, see **Attachment QQQ**. See **Section J, Attachment LLL** for Oracle Middleware Historical statistics.

### C.5.5.6 IMAGE ENGINEERING

The Government will develop the requirements for the content, interaction, and distribution of images to devices and shall update such requirements as needed.

- a. **Image Control Infrastructure:** The contractor shall implement, configure, and maintain a network-accessible data repository for housing and publishing images to desk-side support personnel and other support teams needed. The contractor shall provide all access control management and operations required to ensure appropriate distribution controls of the images. For a list of minimum requirements for the repository, see **Attachment QQQ**.
- b. **Image Engineering - End-User Devices:** The contractor shall develop a set of standard images based on FDIC-defined requirements for use on end-user devices. Each image shall be engineered to include, but is not limited to, the following.
  1. FDIC-defined operating system and version.
  2. A core set of services and functionality to be consistently implemented across all devices of a like type.
  3. A set of services and layered software products to be included in each specific image, based on a profiling assignment for all authorized users.
- c. **Image Engineering – Servers and network devices:** The contractor shall provide management, engineering, and updates for all core images for Windows-based servers, all core images for Unix-based servers, and all core images for Linux-based servers and other network devices, and all layered images for each core images:
  1. For clarity, a core image provides the core operating system, used as the underlying base for a server.
  2. Layered images are core images with a prescribed set of layered software onto the core image for a designated authorized user population or server function.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

- d. **Image Validation and Maintenance:** The contractor shall develop, implement, and execute a test plan for validating each image's proper execution on the specified device. For a list of what the test plan shall include, at a minimum, see **Attachment QQQ**. The contractor shall also develop and implement a process for updating and retesting each image as new versions of software are included, patches are incorporated, and changes are made to configurations. For a list of what the maintenance services shall include, at a minimum, see **Attachment QQQ**.
- e. **Device Image Updating:** The contractor shall develop, implement, and manage a process for "pushing" or allow "pulling" new or revised images to deployed devices. For a list of what this process shall include at a minimum, see **Attachment QQQ**.

### **C.5.5.7 PATCH MANAGEMENT, SERVICE PACK UPGRADES AND PRODUCT UPGRADES**

- a. The Government will provide the following for server hardware and storage sub-systems used in patch management.
  - 1. All utilities required for the continued normal operations of the systems, including electric power and water.
  - 2. Requisite FDIC location work space for support personnel, including desks, telephony, network access, and common areas, restrooms, break areas, and conference rooms.
  - 3. All network data connections to the FDIC WAN / LAN.
  - 4. All server hardware and storage sub-systems used in patch management.
- b. The contractor shall implement, configure, and maintain patch upgrades, servers, and storage subsystems. For a list of procedures that the contractor shall perform, but is not limited to, see **Attachment QQQ**.
- c. **Patch, Service Pack, and Product Upgrade Control Infrastructure:** The contractor shall implement, configure, and maintain a network-accessible data repository for housing and publishing patches, service packs, and product upgrades to desk-side support personnel and other support teams needed. The contractor shall provide all access control management and operations required to ensure appropriate distribution controls of the patches. For a list of minimum requirements associated with this repository, see **Attachment QQQ**.
- d. **Patch, Service Pack, and Product Upgrade Identification:** The contractor shall implement a process for being notified of OEM patches, service packs, and product released for each software package included in all images. This process shall ensure the contractor is aware of new patches within two business days of release by the OEM.
- e. **Patch, Service Pack, Upgrade Evaluation:** The contractor shall evaluate each patch Service Pack, and Product Upgrade released for software packages in the FDIC images for

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

applicability to the end-user environment. For a list of what the evaluation shall include, at a minimum, see **Attachment QQQ**.

- f. **Patch, Service Pack, Product Upgrade Deployment – Scheduled and Emergency:** The contractor shall develop, implement, manage, and maintain a process for testing approved patches and executing a monthly patch Service Pack, and Product Upgrade update to the impacted devices such as, but not limited to, servers, desktops, laptops, network devices, and appliances. The contractor shall also design, engineer, implement, and manage a process and tool set to distribute patches, service packs, and upgrades to end-user devices on an emergency basis. For a list of what the scheduled and emergency patch deployment shall include, see **Attachment QQQ**.
- g. **Patch Frequencies:** The contractor shall provide emergency patches at the following frequencies.
  - 1. Each end-user device shall be eligible to receive an unlimited number of emergency patch updates to mitigate or remove security or performance problems, pushed from the service desk.
  - 2. Each server / mainframe / security / network device shall be eligible to receive an unlimited number of emergency patch updates to mitigate or remove security or performance problems, pushed from the support team either “over-the-wire” or manually installed.
- h. **Patch, Service Packs, Product Upgrade Deployment Verification:** The contractor shall develop, implement, and maintain a tool to check each device on a periodic basis to validate the correct patch, service packs, and product release level is in place. The contractor shall document exceptions and, when required, force a push or manually bring the device to the correct patch level.

### **C.5.6      TASK 6: DEVELOPMENT/QUALITY ASSURANCE/TESTING SUPPORT**

The FDIC IT environment is highly dynamic and must evolve continually to ensure the FDIC maintains the needed levels of IT functionality to serve the public trust. While changes in deployed technologies are common, these changes are generally focused on providing increased productivity and higher levels of security and capacity. The evolution of IT functionality is driven principally through new or revised software. The attentive and technically astute support of the FDIC Development, Quality Assurance, and Test environment(s) is important in maintaining the ability to develop and deploy this new functionality.

Support for the Development/Quality Assurance/Testing support environments requires a holistic view of the FDIC infrastructure. This support model calls for a deep understanding of the FDIC infrastructure and an understanding of application design and business use. This support ensures that planned capabilities, coded in software, are implementable in the FDIC infrastructure and that they will perform as desired without compromising existing capabilities. For

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

Development/Quality Assurance/Testing Support, the contractor provides environment support to the team led by FDIC senior technologists and potentially third-party providers.

In the summer of 2008, FDIC began to implement a new application target architecture called Application Environment Modernization (AEM). It is business-driven and highly integrated with both strategic planning and the current needs of the FDIC. It includes a Service-Oriented Architecture (SOA) that allows the FDIC to assemble applications from shared services within the FDIC. The target architecture fosters the development of common IT services and reuse of IT resources to maximize the return on investment (ROI) for the FDIC. It also promotes interoperability of IT systems and solutions, reducing the investment required for FDIC lines of business to work together collaboratively and efficiently.

This modernized target application architecture at FDIC uses a modular approach for designing and building applications. The target architecture enables the creation and reuse of common application components, solutions that are capability based and can be leveraged by any system needing that capability in reliable, repeatable manner. The target architecture is a multi-layered approach where the presentation layer (client) is separated from the business logic and data access, utilizing a secure, three-tiered architecture.

Since implementing the target architecture, FDIC has been migrating applications from an open Windows and UNIX legacy environment to this new AEM platform. FDIC's application pool consists of hundreds of applications, ranging from COTS products, custom products developed internally, and others like PeopleSoft Financials. FDIC's user community is nationwide. The contractor shall provide expert support for the continued efforts of integrating new and legacy applications to the AEM enterprise environment.

It is important to note that the requirements within this task span the breadth of technologies and IT capabilities at FDIC. Servers, OS, networking, personal computing, middleware, storage, mainframes, and anything on the horizon shall be candidates for support. FDIC will rely on the contractor to provide trained and experienced personnel to meet the ongoing need. Development/Quality Assurance/Test system services are categorized and detailed in the following service sets.

The Government will provide all server, storage, and peripheral equipment and software for Development/Quality Assurance/Test systems, to include Unix, Wintel, and mainframe systems in a controlled, lab environment. The Government will also provide life cycle processes for the proposal, introduction, promotion, evaluation, testing, and release of new or revised products into the FDIC IT production environment, ensuring alignment with all change control processes.

### **C.5.6.1 ENTERPRISE CONTROL PROCESS ALIGNMENT**

The contractor shall provide input, expertise, and advice on enterprise control process development and enhancement to improve the FDIC IT leadership visibility into, control of, and management capability of the FDIC IT environment. In addition, the contractor shall develop all

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

IMS developments and implementations in compliance with FDIC established ITIL and COBIT framework, as expressed and published from the Enterprise Management Services team. Requests for exceptions to FDIC standard processes must be justified in writing with the reason for the exception and shall be approved in writing by FDIC.

### **C.5.6.2 INFRASTRUCTURE SUPPORT**

The contractor shall install, setup, and configure all Government-provided server, storage, and peripheral devices for development / QA / test systems, to include Unix, Wintel, and mainframe systems. The contractor shall also provide advice, leadership, and industry expertise in maintaining and enhancing the development / QA / test infrastructure, to include the following, at a minimum:

- a. Analyze, design, engineer, configure, deploy, and review hardware and software in the FDIC IT environment.
- b. Assist in developing the FDIC IT infrastructure architecture to improve efficiency, stability, and security.
- c. Work with the FDIC enterprise architecture group to develop and enhance architectural directions and plans.
- d. Research, identify, test, and make recommendations for new IT technologies or improved processes for any or all of the existing platforms, systems, or subsystems in existence at FDIC.
- e. Proactively provide detailed review of all IT platforms, systems, and subsystems to ensure all security directives and policies are being adhered to, to evaluate where security enhancements can be made, and provide written results of these reviews.
- f. Develop SOPs for the software installation and deployment process.
- g. Support business continuity and disaster preparedness planning and implementation, systems security vulnerability testing, assessment, and appropriate resolutions for voice, video, and data resources and prepare business continuity and recovery test reports.
- h. Provide support for the operation, maintenance, and administration of current and future call center enterprise software, traffic analysis and network tuning, development and maintenance of operational procedures and network documentation, troubleshooting, reporting, and documenting problems and outages, and assisting with the implementation of network changes

### **C.5.6.3 DEVELOPMENT AND ENGINEERING SUPPORT SECTION (DESS) LAB SUPPORT**

The contractor shall develop policies and procedures for use in the acceptance, installation, activation, support, and promotion of software and hardware into the DESS Lab for quality assurance testing and validation. The contractor shall also install all hardware components and systems, network connections, and associated software (e.g., OS, middleware, applications, databases, layered products, and tooling) on systems in the DESS lab. The contractor shall provide technical support to engineering support personnel in the configuration, test, execution,

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

issue investigation, and establishment of test environments in the DESS lab. For a list of what these policies, procedures, and services shall include, at a minimum, see **Attachment RRR**.

In addition, the contractor shall maintain the capability to provide deep, technical support for all middleware products, technologies, and deployments with FDIC. The contractor shall support middleware for the Oracle, non-database products that are associated with middleware which include Oracle Application Server (OAS) and the related suite of products called 10g; Oracle WebLogic suite of tools (11g) and the Oracle SOA suite. Middleware support's work lies largely in two areas - Application Support and Middleware Activities. With reference to application support, the contractor shall provide assistance to application teams in installation, configuration, deployment and troubleshooting in all environments (production and non-production alike). The contractor shall also provide architectural guidance and assistance. Middleware Activities involve upgrading and patching the Oracle products, monitoring servers for memory, disk usage, and performance. See **Section J, Attachment LLL** for Oracle middleware statistics for 2012. For a list of the minimum on-demand support the contractor shall provide, see **Attachment RRR**.

### **C.5.6.4    INCIDENT/PROBLEM SUPPORT**

The contractor shall ensure productive and responsive support services in Development, QA and Test System support by providing the following support, at a minimum.

- a. Development and maintenance of agreements between teams. Alignment of support team structure to complement application team efforts and to provide an attentive level of support.
- b. Participation in planning and design meetings, where appropriate, to facilitate understanding of project goals and timelines, and to ensure alignment of resources to planned project activities.

The contractor shall actively participate in the identification and resolution of incidents and problems in the Development/QA/Test infrastructure and software. The contractor shall also provide technical support for all technologies, systems, hardware, and software deployed in the Development / QA / Test Environment. For a list of what the minimum support shall include, see **Attachment RRR**.

### **C.5.6.5    APPLICATION SUPPORT**

The contractor shall actively support and actively participate in the development, evaluation, and execution of testing new and/or enhanced applications and functionalities from an infrastructure integration and performance perspective. The contractor shall maintain the capability to provide deep, technical support for all middleware products, technologies, and deployments with FDIC. The contractor shall provide system software maintenance support and software release support. For a list of the minimum requirements associated with these activities, see **Attachment RRR**.



## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

### C.5.7 TASK 7: ASSET ACQUISITION SERVICES (AAS)

The contractor shall provide the following asset acquisition support. The contractor shall develop and execute all asset acquisitions processes in compliance with the FDIC established ITIL and COBIT design principals, as expressed and published from the Enterprise Management Services team. Any exceptions to the process shall be approved by FDIC and documented as to reasoning. The contractor shall provide input, expertise, and advice on enterprise control process development and enhancement to improve the FDIC IT leadership visibility into, control of, and management capability of the FDIC IT environment. The contractor shall actively participate in FDIC-led technical refresh planning efforts and provide information to support the FDIC Procurement Management Board (PMB) meetings. The contractor shall also maintain and publish procurement rosters in support of FDIC planning and service delivery. See **Attachment SSS** for a list of minimum requirements associated with these activities. The contractor shall provide reports according to the specifications contained in **Section J, Attachment G**. The contractor shall also perform the following activities.

- a. The contractor shall develop and implement the required processes and procedures to perform the AAS, to include the following, at a minimum.
  1. Definition of processes for ensuring correct approval of requests.
  2. Integration of connections to FDIC systems for reporting and accounting of expenditures.
  3. Providing a process for rapidly updating approver designation tables (add or remove an approver name, type of asset permitted, or dollar level of authority).
  4. Providing visibility to named FDIC personnel into all AAS actions and documentation.
  5. Tracking classification of contractor source for all procurements.
  6. Tracking of Energy Star and Electronic Product Environmental Assessment Tool (EPEAT) information for hardware purchases.
- b. The contractor shall review and enhance all AAS processes and procedures periodically, to include the following, at a minimum.
  1. Quarterly review of processes for alignment to current FDIC processes.
  2. Timeliness of order processing through receipt of goods and services.
  3. Validity of approver lists and their levels of authority.
  4. Completeness of process in handling requests and processing.
  5. Publish results in a Quarterly AAS Process Review Report (See **Section F, Deliverable 34**).
- c. The contractor shall maintain (update, reformat, validate) and publish procurement rosters in support of FDIC planning and service delivery, to include:
  1. Strategic Roster – roster of non-infrastructure refresh projects for the calendar year that could potentially require the procurement of goods and services along with estimated time of procurement, estimated needs and costing information, and any procurement constraints, or market risks.

## SECTION C – PERFORMANCE-BASED STATEMENT OF WORK

2. Recurring Roster – roster of all maintenance or subscription services with procurement information including estimated costs and timing based upon co-term efforts, maintenance renewals, etc. with a minimal five-year projection.
  3. Procurement Roster – roster of all procurements processed through this TO with breakdown of total expense by category to minimally include: hardware, software, professional services, maintenance, logistics support, delivery schedule, and miscellaneous items.
- d. The contractor shall procure IT-related goods and services for the FDIC in support of the services provided under this requirement. The contractor shall provide all related goods and services documentation in electronic format (e.g., license agreements, terms and conditions, and/or manufacturer specific documentation) (**See Section F, Deliverable 35**). For a list of the types of assets that the contractor may be required to procure, see below.
1. Hardware
  2. Software
  3. Peripherals
  4. \*Evaluation products
  5. Maintenance (individual repairs as well as maintenance agreement contracts)
  6. Telecommunication services
  7. Subscription services
  8. Other IT services
  9. Wireless
  10. BETS telephony
  11. Mobile user subscription and usage
  12. Calling cards
  13. Professional services
  14. Logistics services
  15. Ensure that proof of entitlements, warranties, and other artifacts are registered in the FDIC's name and maintain in accordance with the agreements

\*Note: Evaluation products are typically evaluations of hardware or software products of a similar nature to ensure that the product meets expectations, fits into the overall infrastructure, and performs as the contractor claims. These could be software or hardware assets that are on loan for a period of time and have terms and conditions associated with the handling, timeframe, return, etc.

- e. The contractor shall support analysis of expenditures for content and appropriateness, to include the following, at a minimum:
1. Selected FDIC personnel shall have the ability to access the IMS ticket database to:
    - i. View all issued reports reflecting contractor's performance and the FDIC IT environment.

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

2. Support for invoicing analysis, including (for efficiencies, e.g., consolidations and eliminations):
  - i. Monthly wireless and non-wireless (i.e. wireline) invoice analysis.
  - ii. Monthly mobile user subscription and usage analysis by organization.
  - iii. Maintenance (hardware and software) contract analysis.
3. The contractor shall provide quality assurance review of asset data and records and provide information for the Quarterly Value Audit. Each quarter, FDIC will select a statistically significant sampling of procurements performed by the contractor. The sampling shall be analyzed to ensure the contractor sought the best value (cost / performance) on behalf of FDIC. The contractor shall also provide information on whether or not equipment is under maintenance and/or warranty for specific audit requests.
4. The contractor shall support the formation of bill of material (BOM) documents and data entry support for FDIC executed procurements, to include the following, at a minimum:
  - i. Discuss procurement requirements and maintenance renewals with designated contacts to develop bill of material documents to facilitate acquisition through the contract or by FDIC staff.
  - ii. Facilitate data entry support to minimally include:
    1. Line item entry of all FDIC issued purchase and credit card orders.
    2. Scan and upload procurement artifacts including contracts, invoices, and other contractual correspondence.
    3. Facilitate maintenance of vendor table database within the AMS.
    4. Assist with research efforts related to order logistics.

### **C.5.7.1 ENTERPRISE CONTROL PROCESS ALIGNMENT**

The contractor shall provide input, expertise, and advice on enterprise control process development and enhancement to improve the FDIC IT leadership visibility into, control of, and management capability of the FDIC IT environment. In addition, the contractor shall develop all IMS developments and implementations in compliance with FDIC established ITIL and COBIT framework, as expressed and published from the Enterprise Management Services team. Requests for exceptions to FDIC standard processes must be justified in writing with the reason for the exception and shall be approved in writing by FDIC.

### **C.5.7.2 PROCUREMENT TRACKING SUPPORT**

The contractor shall provide procurement information from the contractor's procurement tracking system on a daily basis. For a list of the type of procurement tracking information that the contractor shall provide, at a minimum, see **Attachment SSS**. The system shall meet the following requirements, at a minimum.

## **SECTION C – PERFORMANCE-BASED STATEMENT OF WORK**

- a. The ability to split each purchase order into multiple lines to accommodate FDIC accounting requirements.
- b. Maintains all accounting data and activities.
- c. Tracks all approved purchases through the procurement life cycle.
- d. Is accessible to FDIC named personnel for data mining and ad hoc report generation.
- e. Aligns to FDIC defined requirements and processes (including the monthly invoicing and accrual processes).
- f. Support for financial audits and ad hoc data requests.
- g. Reports on a calendar year basis and at the TO level, if they are different.

## **SECTION D – PACKAGING AND MARKING**

NOTE: The section numbers in this TO correspond to the section numbers in the Alliant Contract.

### **D.1      PRESERVATION, PACKAGING, PACKING, AND MARKING**

All deliverables submitted to the Government shall indicate the contract number, TO number, contractor's name, description of items contain therein and the consignee's name and address for which the information is being submitted. The contractor shall follow the marking requirements specified by the Government.

## SECTION E – INSPECTION AND ACCEPTANCE

NOTE: The section numbers in this TO correspond to the section numbers in the Alliant Contract.

### **E.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

This TO incorporates the following clauses by reference with the same force and effect as if they were given in full text. Upon request the CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: <https://www.acquisition.gov/far/>

CLAUSE #	CLAUSE TITLE	DATE
52.246-3	Inspection of Supplies – Cost Reimbursement	(May 2001)
52.246-5	Inspection of Services – Cost Reimbursement	(Apr 1984)

### **E.2 PLACE OF INSPECTION AND ACCEPTANCE**

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by FDIC Oversight Manager and the FEDSIM COR.

### **E.3 SCOPE OF INSPECTION**

All deliverables will be inspected for content, completeness, accuracy and conformance to the requirements of this TO by the FDIC Oversight Manager and the FEDSIM COR. Inspection may include validation of information or software through the use of automated tools, testing or inspections of the deliverables or the use of an Independent Verification and Validation (IV&V) contractor. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables according to the Government required standards.

The Government requires a period not to exceed 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

### **E.4 BASIS OF ACCEPTANCE**

The basis for acceptance shall be compliance with the requirements set forth in the TO, the contractor's proposal, and relevant terms and conditions of the Basic Contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses. As well the following acceptance criteria apply to this order:

- a. Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.
- b. If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

Contract Number GS00Q09BGD0025

Task Order GST0013AJ0084

Modification PO12

## **SECTION E – INSPECTION AND ACCEPTANCE**

- c. All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.
- d. If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this TO, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FDIC Oversight Manager and the FEDSIM COR.
- e. For software development, the final acceptance of the software program will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved through documentation updates, program correction, or other mutually agreeable methods.

### **E.5 DRAFT DELIVERABLES**

The Government will provide written acceptance, comments and/or change requests, if any, within 15 workdays (unless specified otherwise in **Section F**) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

### **E.6 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT**

The Government shall provide written notification of acceptance or rejection of all final deliverables within 15 workdays (unless specified otherwise in **Section F**). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

### **E.7 NON-CONFORMING PRODUCTS OR SERVICES**

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor will immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated reduction in the earned award fee.

## SECTION F - DELIVERABLES OR PERFORMANCE

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

### **F.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

This TO incorporates the following clauses by reference with the same force and effect as if they were given in full text. Upon request the CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: <https://www.acquisition.gov/far/>

CLAUSE #	CLAUSE TITLE	DATE
52.242-15	Stop-work Order	(Aug 1989)
52.242-15	Alternate I	(Apr 1984)

### **F.3 TASK ORDER PERIOD OF PERFORMANCE**

The Period of Performance for this TO is a six month base period, five month option period, followed by three one-year and a final seven month optional period.

- Base Period – February 5, 2014 – July 26, 2014
- Option Period 1 – July 27, 2014 – December 31, 2014
- Option Period 2 – January 1, 2015 – December 31, 2015
- Option Period 3 – January 1, 2016 – December 31, 2016
- Option Period 4 – January 1, 2017 – December 31, 2017
- Option Period 5 – January 1, 2018 – July 31, 2018

### **F.4 PLACE OF PERFORMANCE**

The primary place(s) of performance will be at the FDIC Headquarters at Virginia Square in Arlington, VA or at the locations based on the contractor's proposal. Other FDIC locations are contained in **Section J, Attachment F**.

The work locations for the FDIC Washington, D.C. area:

Virginia Square Buildings A, B, C, D, E  
3501 N. Fairfax Drive  
Arlington, VA 22079

Court House Building  
1310 N. Courthouse Road  
Arlington, VA 22079

Contract Number GS00Q09BGD0025  
Task Order GST0013AJ0084  
Modification PO12



## SECTION F - DELIVERABLES OR PERFORMANCE

Downtown Buildings (17<sup>th</sup> Street, F-St., and New York Ave.)  
550 17th Street, NW  
Washington, D.C. 20429

1776 F Street, NW  
Washington, D.C. 20429

1750 New York Avenue  
Washington, D.C. 20006

### **F.5**      **DELIVERABLES**

The following deliverables and timeframes will be used by FEDSIM/FDIC to monitor timely progress on this TO. This schedule is required to meet mission objectives. Variances to this schedule shall be submitted to the COR and CO for approval. The following acronyms apply to this section:

TOA	Task Order Award
IAW	In Accordance With
PMP	Project Management Plan
PS	Project Start
NLT	Not Later Than
OY	Option Year

All days are workdays unless otherwise stated. Deliverables are due the next Government workday if the due date falls on a holiday or weekend. The contractor shall submit the deliverables listed in the following table:

NO	MILESTONE/ DELIVERABLE	TOR REFERENCE	PLANNED COMPLETION DATE
	Project Start		02/05/2014
01	Draft PMP	C.5.1.1.1	PS + 2 weeks
02	Final PMP	C.5.1.1.1	IAW Section E
03	PMP Updates	C.5.1.1.1	IAW PMP
04	Project Kick-Off Meeting	C.5.1.1.2	PS +5
05	Project Kick-off Briefing	C.5.1.1.2	PS + 5
06	Project Kick-off Agenda	C.5.1.1.2	PS + 3
07	Biweekly PMO Meetings	C.5.1.1.2	Biweekly
08	Meeting and Review Minutes	C.5.1.1.2	IAW PMP
09	Monthly Performance Report	C.5.1.1.2	IAW PMP
10	Monthly Financial Report	C.5.1.1.2	IAW PMP
11	Monthly Accrual Report	C.5.1.1.2	IAW PMP
12	Quarterly Spend Plan	C.5.1.1.2	IAW PMP

Contract Number GS00Q09BGD0025  
Task Order GST0013AJ0084  
Modification PO12

## SECTION F - DELIVERABLES OR PERFORMANCE

NO	MILESTONE/ DELIVERABLE	TOR REFERENCE	PLANNED COMPLETION DATE
13	Program Management Web Portal Design	C.5.1.1.3	IAW PMP
14	Program Management Web Portal	C.5.1.1.3	IAW PMP
15	Enterprise Control Process Implementation Plan	C.5.1.2	IAW PMP
16	Technical Refresh Plan	C.5.2.2.1	IAW PMP
17	Disaster Recovery/Business Continuity Plans	C.5.1.4.1	IAW PMP
18	Enterprise Performance Management Approach	C.5.1.5.1	IAW PMP
19	FDIC Asset Management Processes Assessment	C.5.1.7.1	PS + 60
20	License Renew & Tracking Procedures	C.5.1.7.4	IAW PMP
21	AMS Completeness Audit Process	C.5.1.7.7	IAW PMP
22	Training Program	C.5.1.9	IAW PMP
23	Technology White Papers and Briefings	C.5.1.10	IAW PMP
24	Revised Transition-In Plan	C.5.1.11.1	Kick-off Meeting + 10
25	Inventory Status/Reconciliation Report	C.5.1.11.1	NLT the end of in the base period
26	Transition-Out Plan	C.5.1.11.2	120 calendar days after commencement of last OY
27	Maintenance Window Schema	C.5.2.2.2	IAW PMP
28	Electronic Dashboard	C.5.2.2.4	IAW PMP
29	Business Continuity Plans	C.5.2.2.6	IAW PMP
30	Operations Handbook	C.5.2.3.3	IAW PMP
31	Preventive Maintenance Program	C.5.2.6.1	IAW PMP
32	Preliminary Project Plan	C.5.5.2	IAW PMP
33	Service Area Reports	C.5.1.6	IAW PMP
34	Quarterly AAS Process Review Report	C.5.7	IAW PMP
35	Copies of all Purchase Orders /Purchase Request/Subcontracts/ Maintenance & License Agreements	C.5.7	IAW PMP
36	Proposed Necessary Redactions	F.5.1	TOA (or mod) + 10
37	Quarterly Inventory Report	C.5.1.7.8	IAW PMP
38	Semi-Annual Inventory Status Report	C.5.1.7.8	IAW PMP
39	Contractor IT Security Plan	H.7.1.8.2	IAW PMP
40	Gap Analysis and Roadmap	C.5.1.11.1	PS + 60

## SECTION F - DELIVERABLES OR PERFORMANCE

NO	MILESTONE/ DELIVERABLE	TOR REFERENCE	PLANNED COMPLETION DATE
41	EWCC Gap Analysis	C.5.2.2.3	PS + 60
42	Annual Eagle Horizon Business Continuity Exercise	C.5.2.2.6.e	Every June

### F.5.1 PUBLIC-RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the contracting officer's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the Fully Executed Document with all Proposed Necessary Redactions (**See Section F, Deliverable 36**), including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all contractor-proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

### F.5.2 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by email and removable electronic media as well as placing them in the FDIC designated repository. Identified below are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- a. Text                      Microsoft Word
- b. Spreadsheets        Microsoft Excel
- c. Briefings              Microsoft PowerPoint
- d. Drawings             Microsoft Visio
- e. Schedules             Microsoft Project

## SECTION F - DELIVERABLES OR PERFORMANCE

### F.6 PLACE(S) OF DELIVERY

Unclassified deliverables and correspondence shall be delivered to the GSA Contracting Officer's Representative (COR) at the following address:

General Services Administration  
ATTN: Sandy Greenwell, COR  
General Services Administration  
GSA FEDSIM (QF)  
3rd Floor, Wing 1  
1800 F St., NW  
Washington, DC 20405  
Telephone: (703) 589-2564  
Email: sandy.greenwell@gsa.gov

Copies of all deliverables shall also be delivered to the FDIC Oversight Manager at the following address.

FDIC  
ATTN: Joseph Addison  
3501 North Fairfax Dr.  
Arlington, VA 22226  
Telephone: 703-516-5465  
Email: jaddison@fdic.gov

### F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) (**See Section J, Attachment FFF**) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

## **SECTION G – CONTRACT ADMINISTRATION DATA**

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

### **G.3.5 CONTRACTING OFFICER’S REPRESENTATIVE**

The CO will appoint a COR in writing for each TO through a COR Appointment Letter that will be provided to the contractor upon award (Section J, Attachment A). The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

#### **G.3.5.1 CONTRACT ADMINISTRATION**

##### **Contracting Officer:**

Victor Angkico  
General Services Administration  
GSA FEDSIM (QF)  
3rd Floor, Wing 1  
1800 F St., NW  
Washington, DC 20405  
Telephone: (703) 226-9179  
Email: victor.angkico@gsa.gov

##### **Contracting Officer’s Representative:**

Sandy Greenwell  
General Services Administration  
GSA FEDSIM (QF)  
3rd Floor, Wing 1  
1800 F St., NW  
Washington, DC 20405  
Telephone: (703) 589-2564  
Email: sandy.greenwell@gsa.gov

##### **FDIC Oversight Manager:**

Joseph Addison  
FDIC  
3501 North Fairfax Dr.  
Arlington, VA 22226

Contract Number GS00Q09BGD0025  
Task Order GST0013AJ0084  
Modification PO12

## **SECTION G – CONTRACT ADMINISTRATION DATA**

Telephone: 703-516-5465

Email: jaddison@fdic.gov

### **G.9.6 INVOICE SUBMISSION**

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice.

Task Order Number: GST0013AJ0084

Paying Number: A21483282

FEDSIM Project Number: 11044FDM

Project Title: Infrastructure Support Contract (ISC-3)

The contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Tracking and Ordering System (TOS) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

<https://portal.fas.gsa.gov>

Select *Vendor Support*, log in using your assigned ID and password, then click on *Create Invoice*. The TOS Help Desk should be contacted for support at 877-472-4877 (toll free). By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

#### **G.9.6.1 INVOICE REQUIREMENTS**

The contractor shall submit a draft or advance copy of an invoice to the client point of contact (POC) for review prior to its submission to GSA. If the TO has different contract types, each should be addressed separately in the invoice submission. The final invoice is desired to be submitted within six months of project completion.

##### **G.9.6.1.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (FOR LABOR)**

Contract Number GS00Q09BGD0025

Task Order GST0013AJ0084

Modification PO12

## **SECTION G – CONTRACT ADMINISTRATION DATA**

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- a. Employee name (current and past employees)
- b. Employee company labor category
- c. Employee Alliant labor category
- d. Monthly and total cumulative hours worked
- e. Cost incurred not billed
- f. Current approved forward pricing rate agreement in support of indirect costs billed

All cost presentations provided by the contractor shall also include Overhead charges, and General and Administrative charges and shall also include the Overhead and General and Administrative rates being applied.

The Government will promptly make payment of any award fee upon the submission, by the contractor to the FEDSIM COR, of a public voucher and/or invoice in the amount of the total fee earned for the period evaluated. Payment may be made without issuing a TO modification if funds have been obligated for the award fee amount. The contractor shall attach the Award Fee Determining Official (AFDO)/CO determination letter to the public voucher and/or invoice.

### **G.9.6.1.2 COST REIMBURSABLE CLINs (FOR SUBCONTRACOR LABOR)**

The contractor may invoice monthly on the basis of cost incurred for the Cost Reimbursable Subcontractor Labor CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by subcontractor, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- a. Subcontractor Employee name (current and past employees)
- b. Subcontractor Employee company labor category
- c. Monthly and total cumulative hours worked
- d. Cost incurred not billed

All cost presentations provided by the contractor shall also include indirect handling charges applied to subcontractor labor.

## **SECTION G – CONTRACT ADMINISTRATION DATA**

### **G.9.6.1.3 ANCILLARY PRODUCTS AND SERVICES**

The contractor may invoice monthly on the basis of cost incurred for the Ancillary Products and Services CLIN. The invoice shall include the period of performance covered by the invoice and the CLIN number and title and Interagency Agreement (IA) number. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

- a. Ancillary products and services purchased
- b. Consent to Purchase number or identifier
- c. Date accepted by the Government
- d. Associated CLIN
- e. Project-to-date totals by CLIN
- f. Cost incurred not billed
- g. Remaining balance of the CLIN

All cost presentations provided by the contractor shall also include overhead charges, general and administrative charges, and Fee.

### **G.9.6.1.4 TRAVEL**

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
- b. Joint Travel Regulations (JTR), Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.

The invoice shall include the period of performance covered by the invoice, the CLIN number and title, and the IA number. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel details shall include separate columns and totals and include the following:

- a. Travel Authorization Request number or identifier, approver name, and approval date
- b. Current invoice period
- c. Names of persons traveling
- d. Number of travel days
- e. Dates of travel
- f. Number of days per diem charged
- g. Per diem rate used
- h. Total per diem charged

Contract Number GS00Q09BGD0025  
Task Order GST0013AJ0084  
Modification PO12



## **SECTION G – CONTRACT ADMINISTRATION DATA**

- i. Transportation costs
- j. Total charges
- k. Explanation of variances exceeding 10% of the approved versus actual costs
- l. Indirect Handling Rate

All cost presentations provided by the contractor shall also include Overhead charges and General and Administrative charges.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

### **H.1 INCORPORATION BY REFERENCE**

The Contracting Officer reserves the right to incorporate by reference some, all or none of the offeror's proposal. In such instances, the material to be incorporated by reference shall be clearly annotated on the award form, and shall become part of the resultant task order.

### **H.2 KEY PERSONNEL**

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO. Therefore, the Government encourages and will evaluate additional Key Personnel as proposed by the offeror.

- Project Manager
- ISC Chief Architect
- ISC Development/Quality Assurance (QA)/Test Technical Manager
- Client Service Manager (CSM)
- Security Manager
- Data Center Manager
- Engineering Manager
- Asset Manager
- Acquisition Manager

As of Task Order Modification 04, all Key Personnel substitutions shall support ISC-3 on-site at FDIC Monday – Friday. The Government desires that Key Personnel be assigned for the duration of the TO.

#### **H.2.1 PROJECT MANAGER**

The contractor shall identify a full-time single Project Manager (PM) to serve as the Government's primary POC and to provide overall leadership and guidance for all contractor personnel assigned to the TO. The PM is ultimately responsible for the quality and efficiency of the TO to include both technical issues and business processes. The PM shall be an employee of the prime contractor. This individual shall have the ultimate authority to commit the contractor's organization and make decisions for the contractor's organization in response to Government issues, concerns, or problems. This person shall be readily available to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual or programmatic issues.

It is desirable that the PM has the following experience *as a contracted Project Manager* managing Federal and/or state Government environments similar to that of the TO:

Contract Number GS00Q09BGD0025  
Task Order GST0013AJ0084  
Modification PO12

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- a. Demonstrated experience managing and supervising employees in labor categories and with skills applicable to projects similar in size and scope as referenced under this TOR.
- b. Demonstrated experience managing and leading an infrastructure support program with requirements similar to the TOR.
- c. Demonstrated experience managing and upgrading a large, complex, highly available data center operation.
- c. Demonstrated knowledge of commercial hardware and software similar to that of the TOR and the contractor's proposed hardware and/or software.
- d. Demonstrated ability for oral and written communication with the highest levels of management including during the in person question and answer (Q&A) session.
- e. Demonstrated experience managing incentive contracts using acceptable quality levels with incentives and performance metrics.

### **H.2.2      ISC CHIEF ARCHITECT**

The ISC Chief Architect shall lead the translation and estimation of architectural needs into support requirements, including impact on current support operations and capabilities, risk analysis of proposed migrations, and supportability of new technologies. The ISC Chief Architect will be required to support the FDIC with identifying and connecting with industry OEMs and technology leaders; working collaboratively with the FDIC Architecture Lead; and assisting in governance and performance management actions aimed at identifying architecture and technology needs and improving performance of FDIC IT capabilities. It is desirable for the Chief Architect have the following demonstrated experience and/or knowledge:

- a. Demonstrated experience translating organizational architectural needs into requirements, logical designs, physical designs, and tactical construction and deployments.
- b. Demonstrated experience facilitating collaboration with a wide range of OEM and technology leaders.
- c. Demonstrated experience designing, engineering, implementing, and operating enterprise infrastructures similar to what is needed for the FDIC IT environment.

### **H.2.3      ISC DEVELOPMENT/QUALITY ASSURANCE (QA)/TEST TECHNICAL MANAGER**

The ISC Development/QA/Test Technical Manager is responsible for managing the development and testing environments. This person oversees the integration of custom developed applications onto the infrastructure. The Development/QA/Test Technical Manager shall manage the requirements contained in section of the TOR (See **Section C.5.6**). It is desirable that the Technical Manager have the following experience:

- a. Demonstrated experience maintaining and operating a complex IT lab environment, testing life cycles, and following QA principles.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- b. Demonstrated experience implementing technologies, controls, processes, and operational improvements to automate and optimize the management of a development / test lab environment.
- c. Demonstrated experience providing engineering support with requirements similar to the TOR.
- d. Demonstrated ability to work on multiple tasks simultaneously in a high-pressure, mission-critical dynamic environment.
- e. Demonstrated knowledge of technology, architecture, and technical interdependencies similar to that of the TOR.
- f. Demonstrated experience developing and testing a wide range of hardware and software in a lab environment, including anything proposed by the contractor.

### **H.2.4 CLIENT SERVICE MANAGER (CSM)**

The CSM shall lead the technical components of the implementation, operation, and maintenance of the IMS. In addition, the CSM shall manage the technical interfaces between the IMS and other client and supplier systems and lead the development of technical requirements for supplier operating agreements. It is desirable that the CSM have the following experience:

- a. Demonstrated experience managing an enterprise-wide service desk with requirements similar to the TOR, including implementation of ITIL best practices.
- b. Demonstrated experience managing staff with skills applicable to a help desk environment similar in size and scope as referenced in this TOR.
- c. Demonstrated experience managing a 7x24 enterprise-wide service desk.
- d. Demonstrated success improving, optimizing, standardizing, and streamlining customer support processes that yielded improvements in customer satisfaction and resulted in cost reductions.
- e. Demonstrated experience and proven success implementing changes, processes, and standards to improve an enterprise-wide service desk.
- f. Demonstrated experience with help desk technologies and processes as defined in the TOR and as proposed by the contractor.
- g. Demonstrated experience providing performance-based customer service support against multiple performance metrics in the Federal Government.
- h. Demonstrated in-depth experience with the implementation and customization of service desk tools.
- i. Demonstrated advanced proficiency in client services related analysis and project planning.
- j. Demonstrated advanced proficiency with interpersonal and communication skills (verbal and written) in a Federal client services environment similar to the TOR.

### **H.2.5 SECURITY MANAGER**

The Security Manager is responsible for managing the infrastructure that supports the DIT Information Security Program. It is desirable for the Security Manager to have the following experience:

Contract Number GS00Q09BGD0025  
Task Order GST0013AJ0084  
Modification PO12

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- a. Demonstrated experience in planning, directing, and managing complex IT projects from a security context of a nature similar in size and scope as referenced in the TOR.
- b. Demonstrated experience providing detailed security technical leadership to security employees of various labor categories and skills in telecommunications on IT projects of similar in size and scope as referenced in the TOR.
- c. Demonstrated experience with technical and administrative leadership of task compliance with industry accepted standard.
- d. Knowledge of encryption devices, certification and accreditation concepts, and security procedures as would be required in this TOR.
- e. Knowledge of network and system operation, to include network and system security.
- f. Demonstrated ability for oral and written communication with higher levels of management.
- g. Demonstrated ability to manage multiple tasks simultaneously in a high-pressure, mission-critical, secure environment.

### **H.2.6      DATA CENTER MANAGER**

The FDIC DIT maintains a primary and a secondary data center which should be considered complex, in that it supports all classes of servers, storage, databases, networking, applications, and security. At a minimum, the Data Center Manager shall develop a strategy of operation that is consistent with and leverages industry best practices while supporting the U.S. Government and FDIC Security Disciplines. The Data Center Manager must implement standards, processes, controls, and discipline across the operation to deliver reliable and consistent services. It is desirable for the Data Center Manager to have the following demonstrated experience:

- a. Demonstrated experience managing Data Center Operations similar in size, complexity, dynamics, availability and scope to that of the TOR.
- b. Demonstrated experience managing mainframe and server Physical and logical security, Disaster recovery failover, business continuity, and Batch job scheduling in mainframe and distributed (i.e., Windows and Unix) operating system environments.
- c. Demonstrated experience managing large, complex server environments containing over 500 physical servers that host over 1,500 physical or virtual servers.
- d. Demonstrated experience planning and executing server consolidation and virtualization efforts on Windows, Solaris, and Red Hat Linux in a production operational environment.
- e. Demonstrated experience managing enterprise class storage across server technologies (e.g., Windows, Solaris, Red Hat, VMware) implementing operational best practices, provisioning standards, and storage migrations and optimizations.
- f. Demonstrated experience with implementing ITIL standards and processes in a large, highly available, dynamic data center operation.
- g. Demonstrated experience managing a 7x24 command center that monitors a national service and manages faults and failures proactively and reactively.
- h. Demonstrated experience managing IBM Z10 mainframe with z/OS Operating System.
- i. Demonstrated experience translating between business requirements and technical implementation.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- j. Demonstrated experience with systems engineering in the context of a large, complex infrastructure.

### **H.2.7 ENGINEERING MANAGER**

The Engineering Manager is responsible for overseeing and managing all engineering projects. This person plays a critical role in the strategic planning of the infrastructure and building a resilient architecture. It is desirable for the Engineering Manager to have the following demonstrated experience:

- a. Demonstrated experience providing engineering support with requirements similar to the TOR. This includes, but is not limited to, implementing new server, network, storage, backup, and management technologies that introduce efficiencies, optimizations, and improved delivery of services.
- b. Demonstrated experience implementing technical and process change in a highly complex infrastructure similar to the FDIC to introduce new technologies and processes to improve availability, management, monitoring, support, patching, and scalability.
- c. Demonstrated experience working collaboratively with the architects, development leads, and operations to glean requirements and needs to design and provision infrastructure capabilities that yield a flexible environment that supports the known business and technical requirements to include servers, storage, network (LAN, SAN, WAN, internet), monitoring, backups, automation, patching, and scalability.
- d. Demonstrated experience managing and leading an engineering staff with skills applicable to a project environment similar in size and scope as referenced in this TOR.
- e. Demonstrated experience in providing the leadership for prioritizing, planning, and successfully delivering multiple projects in parallel and in cooperation with a production environment with a large engineering and operations staff.
- f. Demonstrated expertise for providing management for oral and written communication with the highest levels of management while providing technical leadership to engineering and operational teams.
- g. Demonstrated experience with development, implementation, and optimization of technology life cycle processes

### **H.2.8 ASSET MANAGER**

The Asset Manager has overall responsibility throughout the life cycle of the assets. The safeguarding of the assets and the integrity of the data around them is a critical aspect of this responsibility. It is desirable for the ISC Asset Manager to have the following demonstrated experience:

- a. Demonstrated experience in IT, with experience as a service delivery technical lead for an asset management services program involving the management of a diverse asset inventory across multiple geographic locations.
- b. Demonstrated in-depth experience leading teams and projects in the implementation and customization of asset management tools and processes. This includes standards and

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

processes for automation for receiving assets, maintaining a reliable asset management system, conducting inventories, developing and implementing processes to implement automation and standards that yield consistent results and rigor in asset management throughout the life cycle.

- c. Demonstrated expertise in managing the full asset life cycle including acquisition, deployment, repair, upgrading, and retirement processes from business, industry, and governing perspectives.
- d. Demonstrated proficiency in asset management analysis and project planning.
- e. Demonstrated proficiency with interpersonal and communication skills (verbal and written).

### **H.2.9 ACQUISITION MANAGER**

The Acquisition Manager manages the procurement process for all acquisitions obtained by the contractor. This person facilitates renewals of maintenance and support services contracts to ensure availability of post-warranty support and software upgrade entitlements; resolves warranty disputes and product returns; and identifies and reports market challenges or trends that may prevent timely acquisition of goods and services.

It is desirable for the Acquisition Manager to have the following demonstrated experience working on Federal acquisitions:

- a. Demonstrated experience in implementing organizational process and disciplines in the management of large and small information technology acquisitions (totaling approximately \$150M per year) in support of Federal Government clients.
- b. Demonstrated proficiency in asset management analysis and project planning.
- c. Demonstrated proficiency with interpersonal and communication skills (verbal and written).
- d. Demonstrated experience analyzing organizational IT procurements, identifying opportunities to reduce costs through innovative procurement vehicles, reducing service / support levels to procure necessary support to deliver organizational needs, analyzing inventory in order to reduce the number of maintenance and support agreements.
- e. Demonstrated expertise in working collaboratively with IT management and executives to deliver financial / cost analysis.

### **H.2.10 KEY PERSONNEL SUBSTITUTION**

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a TOR, the contractor shall notify the Government CO and the COR of the existing TO. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6, Termination (Cost Reimbursement) or FAR 52.249-8, Default (Fixed-Price Supply and Service).

### **H.2.11 NON-KEY PERSONNEL REQUIREMENTS FOR FUNCTIONAL LEADS**

The contractor shall provide the following functional categories in their staffing plan. The Government is looking for a set of highly knowledgeable and qualified staff to support this TO in lead positions. During the transition period and in accordance with the contractor's Government-approved Transition-in Plan, the contractor shall provide named (i.e., names required to be provided to the Government only after award) personnel for the following functional categories. After award, the Government will evaluate (within the parameters of the AFDP) the quality of the provided personnel by measuring the contractor's ability to meet the Government's service-level metrics (See **Section J, Attachment D**).

The contractor may choose, on its own discretion, to propose none, any, or all of the following functional leads as additional Key Personnel (See **Section L.8.3**). In that case, they must be named and will be evaluated according to the Key Personnel criteria in **Section M.5.2**.

#### **H.2.11.1 FINANCIAL LEAD**

It is desirable for the Financial Lead to have the following demonstrated experience:

- a. Demonstrated experience in accounting and / or corporate finance for large corporate or government organizations to include managing the invoicing / finances for \$150+ MM (annually) IT outsourcing programs.
- b. Demonstrated ability to quickly respond to client requests and resolve invoicing errors or generate reports.
- c. Demonstrated working knowledge of financial systems.
- d. Demonstrated communications and problem solving skills.
- e. Demonstrated experience with leveraging financial management systems where analysis and reporting can be developed and delivered to management.

#### **H.2.11.2 SERVER MANAGEMENT TECHNICAL LEAD**

It is desirable that the Server Management Technical Lead have the following qualifications:

- a. Demonstrated proficiency in storage management analysis and project planning.
- b. Demonstrated proficiency in with interpersonal and communication skills (verbal and written) to include advising engineering, operations, and management organizations on server systems design, architecture, and engineering.



## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- c. Demonstrated expertise serving as a technical expert and manager for all servers (Windows, UNIX - Solaris, Linux – Red Hat, and Mainframe – z/OS) operations and maintenance, to include developing and implementing tools and process to standardize and automate the provisioning, management (backups, upgrades, patches, and drivers), monitoring of systems and services, and leveraging industry best practices to include clustering, workload balancing, redundancies for LAN & SAN.
- d. Demonstrated expertise constructing, testing, and maintaining software packages to enable the automated and consistent construction of servers.
- e. Demonstrated expertise with deployed server platforms, including device and software configurations and working collaboratively to design, provision, and maintain test environments, and the evaluation of new configurations, patches, upgrades, and image modifications.
- f. Demonstrated expertise with the design, deployment, integration, migration, and operation of virtualization technologies and applications on Intel and SUN hardware platforms.
- g. Demonstrated expertise with defining and implementing comprehensive server monitoring, encryption, and security assurance technologies.
- h. Demonstrated expertise maintaining vivid awareness and understanding for the technical direction and industry trends to support organizational strategy planning, as well as to support server designs, that enable FDIC to leverage new services and technologies that have been announced in vendor plans and roadmaps.

### **H.2.11.3 SERVICE DESK TECHNICAL LEAD**

It is desirable that the Service Desk Technical Lead have the following qualifications:

- a. Demonstrated expertise delivering end user support to assist with using and resolving problems with the software and device technologies supporting FDIC.
- b. Demonstrated experience with implementing incident workflow in a customer service environment to maintain continuous customer contact wherever possible.
- c. Demonstrated experience with technical interfaces between an IMS and client and supplier systems.
- d. Demonstrated success developing, implementing, and maintaining technical requirements for supplier operating agreements.
- e. Demonstrated experience as a service delivery technical lead for a complex service desk implementation.
- f. Demonstrated in-depth expertise in the implementation and customization of the supplier service desk tools to include trouble ticket management, call routing, call queue management, and call escalation.
- g. Demonstrable experience in the development and implementation of client-specific change control processes/workflows and follow-up on customer problems through closure and customer satisfaction resolution.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

### **H.2.11.4 STORAGE MANAGEMENT TECHNICAL LEAD**

It is desirable that the Storage Management Technical Lead have the following qualifications:

- a. Demonstrated success and expertise in the designing of storage to the component level, leading the implementation, provisioning, and operation of storage technologies that are in accordance with industry and contractor standards, processes, and best practices.
- b. Demonstrated understanding of storage provisioning to support system, database, and application requirements, as well as experience working collaboratively with teams to support the operations and maintenance of the services.
- c. Demonstrated expertise and comprehensive knowledge of replication, backup, and snapshot technologies and capabilities by contractor and product to deliver flexible and optimal services and solutions to support business and application requirements.
- d. Demonstrated expertise and with implementation of storage virtualization technologies and applications such as storage pools, automated storage tiering, and thin provisioned allocations while ensuring that all designs and implementations support resilience and high availability.
- e. Demonstrated success and implementation of monitoring and management systems to proactively manage capacity, availability, and health of all components in the storage infrastructure.

### **H.2.11.5 WAN/MAN (DATA NETWORKS) TECHNICAL LEAD**

It is desirable that the WAN/MAN (Data Networks) Technical Lead have the following qualifications:

- a. Demonstrated in-depth expertise and proven success in the implementation and customization of network management and performance tooling.
- b. Proven success leading the design, architecting, engineering, upgrading, and troubleshooting of a large enterprise production WAN and Metropolitan Area Network (MAN) carrying data, video, and voice traffic and managing a converged Multiprotocol Label Switching (MPLS) network carrying voice, data, and video traffic.
- c. Proven delivery of a secured wireless network for a large corporation or government agency.
- d. Hands on and thorough expertise and understanding of WAN / MAN devices and their configurations, including, but not limited to, routers, switches, and firewalls.
- e. Demonstrated expertise advising on technology innovations and industry trends to support the delivery of new capabilities that provide greater flexibility, improved availability, converged services, reduced costs, while providing security technologies to mitigate threats.
- f. Proven and detailed understanding of the software and device supporting Network Monitoring Tools (NMT), and the monitoring / reporting capabilities of the NMT.

### **H.2.11.6 LAN AND REMOTE ACCESS TECHNICAL LEAD**

It is desirable that the LAN and Remote Access Technical Lead have the following qualifications:

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- a. Demonstrated leadership in network analysis to support the methodical and careful delivery of new LAN technologies with minimal disruption to production operations. This includes developing detailed project plans, negotiating schedules, leveraging interpersonal and communication skills (verbal and written) to execute the delivery of new services and supporting the enhancing and troubleshooting of existing services.
- b. Demonstrated experience serving as a technical expert and manager for LAN and remote access design, architecture, engineering, operations, and maintenance and an understanding of LAN and remote access devices and their configurations, including, but not limited to, switches, routers, wireless access points, and firewalls in a large corporation or a government agency with over 10,000 employees and over 75 locations that span the country.
- c. Proven success and detailed understanding of the software and devices supporting NMT, and the proactive and reactive monitoring / reporting capabilities of the NMT in a large operational corporation or government agency.

### **H.2.11.7 TELEPHONY (VOICE/VOIP) TECHNICAL LEAD**

It is desirable that the Telephony (Voice/VoIP) Technical Lead have the following qualifications:

- a. Demonstrated experience serving as a technical expert in the implementation, management, upgrade, and customization of enterprise Voice / VoIP Avaya voice system management, performance tooling and operations and maintenance.
- b. Demonstrated knowledge of maintaining understanding of emerging telecommunications and voice emerging technologies.
- c. Demonstrated experience providing and developing methodical and detailed plans for system upgrades that include test plans, back out plans, communication plans, voice technology innovations, voice security threats, and other industry trends.
- d. Demonstrated experience thorough expertise and understanding of Voice / VoIP Devices and their configurations, including, but not limited to, PBXs, switches, routers, mailbox systems, and handsets.
- e. Demonstrated experience understanding of the software and device supporting NMT, and the monitoring / reporting capabilities of the NMT for voice systems to proactively and reactively address problems in a large production multisite operation supporting over 10,000 employees.

### **H.2.11.8 WEBCASTING, WEB CONFERENCING & VTC TECHNICAL LEAD**

It is desirable that the Webcasting, Web Conferencing & VTC Technical Lead have the following qualifications:

- a. Demonstrated experience serving as a technical expert and manager for all webcasting, web conferencing, and VTC operations and maintenance to include the implementation and customization of webcasting, web conferencing and VTC systems and capabilities.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- b. Demonstrated experience leading the analysis of requirements, developing engineering plans, providing technical leadership to implement the plans and possessing the negotiating, interpersonal, and communication skills (verbal and written).
- c. Demonstrated experience operating and managing webcasting, web conferencing, and VTC devices and their configurations, including, but not limited to, displays, video cameras, audio equipment, telepresence equipment, and projectors.
- d. Demonstrated and detailed understanding of the software and device supporting NMT, and the monitoring / reporting capabilities of the NMT for all components and services that are delivered by the team to include proactive and reactive monitoring as well as capacity and performance.

### **H.2.11.9 SENIOR WINDOWS ENGINEER/LEAD**

It is desirable that the Senior Windows Engineer/ Lead have the following qualifications:

- a. Demonstrated experience in designing, engineering, implementing, and supporting medium to large scale of Microsoft 2000 / 2003 /2008 Windows Servers environment (more than 1,000 servers and over 10,000 users) and Active Directory, SQL server, IIS server, and a plethora of custom applications.
- b. Knowledge of networking topology and protocols and network management.
- c. Demonstrated experience developing high-level and detailed infrastructure designs of Microsoft-based solutions such as MSSQL, PKI, SharePoint, Search, SCOM, Exchange, SCCM, and others.
- d. Demonstrated experience taking technical requirements and developing the technical solutions and providing technical expertise, detailed project planning, and implementation and operational deployments, support, upgrades, and troubleshooting.
- e. Demonstrated experience developing process to standardize and automate standard tasks to install discipline and consistency.
- f. Demonstrated experience managing Windows servers in a VMWare environment.
- g. Demonstrated experience supporting and automating the rigorous patching of servers distributed across the country to maintain security and best practices.

### **H.2.11.10 SENIOR MESSAGING ENGINEER/LEAD**

It is desirable that the Senior Messaging Engineer/Lead have the following demonstrated experience:

- a. Demonstrated experience in designing, engineering, implementing, and supporting enterprise messaging systems to include Microsoft Exchange 2010 in a medium to large enterprise (more than 10,000 users).
- b. Demonstrated experience understanding and troubleshooting messaging protocol and architecture including related components such as mobile messaging (Blackberry, ActiveSync).

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- c. Demonstrated experience working experience in Microsoft Windows Server 2008 and Active Directory and related Microsoft collaboration technology and solutions such as Live Meeting, Communications Servers, and Collaboration SharePoint.
- d. Demonstrated working knowledge of enterprise storage (SAN/NAS) and virtualization (VMware) is preferred.

### **H.2.11.11 SENIOR UNIX/LINUX ENGINEER/LEAD**

It is desirable that the Senior Unix/Linux Engineer/Lead have the following demonstrated experience:

- a. Demonstrated experience in designing, engineering, implementing, and supporting UNIX (Solaris) and Linux (Redhat) servers and enterprise application.
- b. Demonstrated experience in building, configuring, and optimizing enterprise UNIX servers (Oracle/Sun M series of above) with associated virtualization and clustering technology.
- c. Demonstrated hand-on working experience with Redhat Enterprise servers in a VMware cluster environment.
- d. Demonstrated knowledge of Enterprise Storage (SAN/NAS) and Virtualization (VMware).

### **H.2.11.12 SENIOR DESKTOP ENGINEER/LEAD**

It is desirable that the Senior Desktop Engineer/Lead have the following demonstrated experience:

- a. Demonstrated experience in designing, engineering, implementing, and supporting desktop engineering and deployment.
- b. Demonstrated hands-on experience in desktop imaging and software distribution in a medium or large environment (more than 10,000 desktops).
- c. Demonstrated working knowledge of desktop security patch deployment.

### **H.2.11.13 SENIOR STORAGE ENGINEER/LEAD**

It is desirable that the Senior Storage Engineer/Lead have the following demonstrated experience:

- a. Demonstrated experience in designing, engineering, implementing, and supporting enterprise storage technology and solutions: SAN/NAS from the major contractors such as EMC, Netapps, Hitachi, etc.
- b. Demonstrated ability to manage large enterprise storage environments (more than two Petabyte of storage).
- c. Demonstrated knowledge and hands-on skill sets in configuring and optimizing storage with remote replications and backup.
- d. Demonstrated working knowledge of virtualization (VMware, Microsoft) is also desired.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

### **H.2.11.14 SENIOR VOICE/VIDEO ENGINEER/LEAD**

It is desirable that the Senior Voice/Video Engineer/Lead have the following demonstrated experience:

- a. Demonstrated experience in designing, engineering, implementing and supporting Voice/Video in a mixed PBX/VoIP environment.
- b. Demonstrated experience in configuring and Avaya PBX and VoIP and Tandberg video conference systems for medium to large enterprise with nationwide, remote offices.

### **H.2.11.15 SENIOR NETWORK ENGINEER/LEAD**

It is desirable that the Senior Network Engineer/Lead have the following demonstrated experience:

- a. Demonstrated experience in design, engineering, implementing, and supporting telecommunications and data network for medium to large enterprise with multiple remote offices nationwide.
- b. Demonstrated experience in routing and switch technology and protocol (Cisco Certified Internetwork Expert (CCIE) is preferred).
- c. Demonstrated hands-on experience in designing robust and redundant MAN, MPLS-based WAN and LAN in a mixed network equipment contractors such as Cisco, Juniper, etc.
- d. Demonstrated working knowledge of security engineering and technology such as firewall, IDS, encryption appliance.

## **H.4 CONTRACTOR TRAINING**

The contractor is generally expected to maintain the professional qualifications and certifications of its personnel through on-going training. Unless specifically authorized by the Government, the contractor shall not directly bill the Government for any training.

## **H.5 GOVERNMENT-FURNISHED PROPERTY/SPACE (GFP/S)**

If the offeror's proposal plans to be an onsite implementation, then the Government will provide standard office space and accessories as Government-Furnished Property (GFP) for contractor personnel at the following location: Federal Deposit Insurance Corp., 3501 Fairfax Drive, Arlington, VA 22226, and other locations as determined necessary and acceptable to the Government. Contractor staff will be assigned to specific room and office locations in the above facility as soon as possible following contract award. FDIC is in the process of hiring additional Federal staff that will be located at the Virginia Square facility. As Federal staff increases, space for contractors will decrease.

The Government will furnish the following as GFP: 1) computers, 2) printers, 3) office space, and 4) telephones (land lines & Blackberry device for selected operational personnel) for the contractor staff listed below.

Contract Number GS00Q09BGD0025

Task Order GST0013AJ0084

Modification PO12

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

If the offeror's proposal plans to be an offsite implementation, then:

The Government will furnish the following as GFP: 1) computers, 2) Blackberry devices for selected operational personnel, 3) a communications line to the primary location of offsite personnel, and 4) necessary communication equipment to meet FDIC security requirements.

If the offeror's proposal plans to include some outside service implementation, then:

The Government will furnish the following as GFP: 1) communications line to the primary location of outside service, and 2) necessary communication equipment to meet FDIC security requirements.

All other GFP provided by the Government that is not specified above is detailed in the applicable attachment in Section J and will be provided during transition in.

The Government will provide a small amount of asset storage space at each Regional/Field site. The Government will also provide contractor desk space for the following number of people by site:

Atlanta, Georgia	1 person
Boston, MA	1 person
Chicago, IL	1 person
Dallas, TX	15 people
Washington, DC/VA	280 people
Jacksonville, FL	6 people (scheduled to close by April 2014)
San Francisco, CA	<u>1 person</u>
Total	305 people

The Government will also provide the following space at the DDC for contractor usage:

### **P1 (1082)**

1721.25 sq. ft.

Length – 67.5 ft.

Width – 25 ft.

### **P1(1107)**

483 sq. ft.

Length – 23 ft.

Width – 21 ft.

### **P2 (Bulk Storage)**

2501.25 sq. ft. (with fence)

Length – 57.5 ft.

Contract Number GS00Q09BGD0025

Task Order GST0013AJ0084

Modification PO12

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

Width – 43.5 ft.

Pillar to Pillar – 30 ft. (current fence pillar to additional space pillar)

Length – 57 ft.

Width – 30 ft.

1725 sq. ft. + 2501.25 sq. ft. = 4226.25 sq. ft. (without fence)

The environment should be maintained between 68 and 80 degrees Fahrenheit with humidity levels between 45 – 60%.

The Government will also provide for contractor usage, the hardware and software indicated in the **Section J.1** attachments.

### **H.5.2      GOVERNMENT-FURNISHED INFORMATION (GFI)**

See **Section J.1**.

### **H.7.1      FDIC GENERAL SECURITY REQUIREMENTS**

#### **H.7.1.1    PERSONAL SECURITY**

##### **H.7.1.1.1 SECURITY CLEARANCE**

The contractor personnel who are working on sensitive or confidential projects to be security cleared first before allowing them to work on any FDIC services. All contractor personnel (prime and subcontractor) who require high level risk designation must be a US Citizen. The clearance requirements shall comply with the security level determined by the system owner, the FDIC and the relevant Federal government authority.

The offeror shall submit the following documents to the FDIC Oversight Manager (Section G.3.5.1) for all Key Personnel two days after TOA. After this milestone the contractor shall submit the following documents for all personnel (prime and sub) to include key personnel substitutions.

- Background Investigation Questionnaires for Contract Personnel and Subcontractors (FDIC 1600/4) (Section H.7.1.8.11 and Section J, Attachment AAA)
- Notice and Authorization Pertaining to Consumer Reports (FDIC 1600/10) (Section H.7.1.8.11 and Section J, Attachment XX)
- Questionnaire for Public Trust Positions (SF 85P) (Section J, Attachment VVV)
- Personnel Security Action Request (FDIC 1600/13) (Section J, Attachment WWW)
- Employee/Contractor Identification Card Request (1620/01) (Section J, Attachment XXX)



## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- Declaration of Federal Employment, Submission Requirements for Contractor Personnel (Optional Form (OF)-306) (Section J, Attachment YYY)
- Additional Background Security Questions for Contractor Personnel (FDIC 1600/25) (Section J, Attachment ZZZ)

### **H.7.1.1.2 BACKGROUND INVESTIGATIONS**

- a. Background investigations will be conducted for all contractor and subcontractor personnel. The extent of the investigations will be in direct relation to the risk level assigned to the contract or to the individual job classifications.
- b. Each contractor and subcontractor employee working on the contract must complete an electronic fingerprint application and credit report authorization. No employee will be permitted to begin work (including access to FDIC facilities, network, and systems) until a favorable fingerprint records check and credit report has been received by the FDIC, unless an FDIC waiver has been obtained.
- c. The FDIC Oversight Manager (OM) must obtain preliminary background investigation approval of the contractor and Key Personnel from Security and Emergency Preparedness Section, immediately after award and prior to project start. This approval is required when the award exceeds \$100,000 and is for services or at any dollar amount when contractor personnel or subcontractor personnel work on-site and have unescorted access to FDIC offices or facilities, or have access to FDIC networks/systems or in any other contract where the Program Office has described a need for background investigations. (See Section J, Attachment MMM for the current version of FDIC's Acquisition Procedures, Guidance and Information (PGI) document; dated March 2011; updated versions (as supplemented by new and revised provisions and clauses), may be found at: <http://www.fdic.gov/buying/goods/acquisition/index.html>)
- d. Within 30 days after award hereof, the contractor must provide the FDIC OM with a list of all contractor and subcontractor personnel proposed for work on the contract. This list must include the employee's name, current home address, and assigned risk level. The contractor must identify each employee who has a previous current or otherwise valid background investigation, and such background investigations must be furnished to FDIC with the list of personnel.
- e. For those employees of the contractor or subcontractor who do not possess a valid FDIC background investigation, a background investigation will be conducted for them. In that event, the requirements relating to background investigations contained herein will control.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- f. NOTE: A valid background investigation is one that meets the minimum investigation for the risk level established for the TO or TO job category, and that has been conducted within 5 years of the date of TOA.
- g. Any adverse findings identified during the background investigation or fingerprinting review (e.g., felony conviction), or a completed background investigation or fingerprint check that indicates that an employee cannot meet the designated security requirements, may affect the TO. The contractor and/or subcontractor with compliance conflict may be removed at the discretion of the agency and replaced with an employee acceptable (limited to their background investigation) to FDIC by the contractor at no additional expense to FDIC and without relief in all contractual performance and delivery requirements. Any additional employees hired after TOA are required to comply with the same process as noted above.
- h. All contractor and subcontractor employees regularly working on-site at an FDIC facility will be issued a yellow identification/access control badge. Such employees will not be granted on-site access until FDIC receives a favorable fingerprint criminal records check from the FBI. The badges will be issued for a six-month period and must be renewed after each six-month period.
- i. Contractor must notify the FDIC OM of any new contractor or subcontractor personnel assigned to the contract or any change in assignment of current personnel. FDIC will perform the appropriate background investigations and fingerprint check for any such personnel.

### **H.7.1.1.3 RISK LEVEL DESIGNATION (ENTIRE CONTRACT), 7.5.2-9 (PGI)**

The risk level for this contract is HIGH. The post-award background investigations for this contract will be done at this risk level.

### **H.7.1.1.4 RISK LEVEL DESIGNATION (LABOR CATEGORY) (JULY 2008), 7.5.2-10 (PGI)**

The contractor shall provide risk/level designation by labor category to support all post-award background investigations.

### **H.7.1.1.5 RISK LEVEL DESIGNATION**

The post-award background investigations and fingerprinting required for all contractor employees (and subcontractor employees, if applicable) will be based on the risk level assigned by the FDIC to each type of work being performed. In accordance with FDIC Circular 1610.2, the risk level for the types of work will be determined, based on the apparent successful proposal, prior to task award. The definition of the various risk levels that can be found in the

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

FDIC Directive titled Security Policy and Procedures for FDIC contractors and Subcontractors at <http://www.fdic.gov/formsdocuments/1610-2.doc>.

### **HIGH RISK LEVEL - Definition**

The contractor's duties or responsibilities are especially critical to the Corporation (FDIC) or its program mission, systems, or information with a broad scope of policy or program authority (e.g., policy development and implementation; higher level management assignments; independent spokesperson; or non-management positions with authority for independent action). Contractor has access to highly sensitive/critical systems or information with the potential for causing exceptionally serious damage.

#### **Job Responsibility Examples:**

1. Responsibility for the development, implementation, and/or administration of FDIC computer security programs.
2. Significant involvement in life-critical or mission critical systems or programs.
3. Responsibility for preparing or approving data for input into a system which does not necessarily involve personal access to the system, but which creates a high risk for effecting grave damage or realizing significant personal gain.
4. Responsibility for the planning, design, testing, maintenance, operation, monitoring or management of systems hardware or software.
5. Access to a system during the operation or maintenance in such a way to permit high risk for causing grave damage or realizing significant personal gain.
6. Work involving investigative, compliance, or senior level auditing type duties.
7. Access to sensitive financial information which could result in realizing significant personal gain.
8. Significant public health or public safety duties.
9. Access to or control of highly sensitive, but unclassified information/data.
10. Work involving fiduciary, public contact, or other duties involving the highest degree of public trust.
11. Work occurring after duty hours within FDIC buildings which are not supervised by an FDIC employee and where appropriate physical security measures are not in place to prevent unauthorized access to sensitive data or information.
12. Any other duties designated by the FDIC OM which will have a high risk for effecting grave damage or realizing significant financial gain.

### **MODERATE RISK LEVEL - Definition**

The contractor's duties or responsibilities are of considerable importance to the Corporation or particular program mission, system(s), or information. Contractor has access to moderately sensitive/critical systems or information with the potential for causing moderate damage.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

### **Job Responsibility Examples:**

1. Work involving similar duties as outlined in the high risk job responsibility examples identified above, but which has close technical review by a senior FDIC employee.
2. Work involving free access and movement within FDIC buildings during normal duty hours with little or no supervision by an FDIC employee.
3. Work occurring after duty hours within an area which houses sensitive information or equipment even though supervised by an FDIC employee.
4. Work requiring access to sensitive information such as that protected by the Privacy Act.
5. Any other duties designated by the FDIC OM.

### **LOW RISK LEVEL - Definition**

The contractor's duties and responsibilities have limited impact on the Corporation or particular program mission, system(s), or information. Contractor has access to systems or information with the potential for causing minimal damage.

### **Job Responsibility Examples**

1. All other duties/responsibilities not falling into the Moderate or High job responsibility examples identified above.

#### **H.7.1.1.6 PERSONNEL BADGING**

The contractor shall provide a list of contractor personnel that require expedited FDIC badging and security clearances. The Government will expedite such badging and security clearances for the contractor staff after award provided the individuals meet the necessary security qualifications. The Government will grant contractor personnel access to the FDIC sites, subject to compliance with security and safety requirements, within 60 days of TOA.

#### **H.7.1.1.7 COMPLIANCE WITH THE PERSONAL SECURITY REQUIREMENTS**

The contractor shall comply with the following:

- FDIC Circular 1610.2, Personnel Security Policy and Procedures for FDIC Contractors, (See Section H.7.1.8.13)
- Access to FDIC Information Systems (June 2010), 7.5.1-3 (PGI), (See Section H.7.1.8.7)
- Contractor Security Training, (See Section H.7.1.3.2)
- 12, CFR, PARTS 366, 377 (See Section H.7.1.8.10)
- Background Investigation Questionnaires, 7.5.2-1 (PGI), (See Section H.7.1.8.11)
- Background Investigations, Alternate 1 (May 2009), 7.5.2-3 (PGI), (See Section H.7.1.8.12)
- Risk Level Designation (Entire Contract), 7.5.2-9 (PGI), (See Section H.7.1.1.3)
- Risk Level Designation (Labor Category) (July 2008), 7.5.2-10 (PGI), (See Section H.7.1.1.4)

Contract Number GS00Q09BGD0025

Task Order GST0013AJ0084

Modification PO12

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- Identification/Access Badges, 7.5.2-11 (PGI), (See Section H.7.1.8.8)
- Use of FDIC Premises by Contractor Personnel, 7.5.2-13, (See Section H.7.1.8.9)

### **H.7.1.2 ACCESS CONTROL**

#### **H.7.1.2.1 SYSTEM ACCESS**

The contractor shall allow FDIC, including the Office of Inspector General, access to the contractor's and all subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the TO. Access shall be provided to the extent required to carry out a program of IT inspection, investigation and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of FDIC data, systems, software and hardware or to the function of computer systems operated on behalf of FDIC or the network accessed by the contractor personnel and to preserve evidence of computer crime or misuse.

Access to FDIC systems will be granted in accordance with the FDIC's System Access Procedures. All data and system software is the property of the FDIC and may only be used in the performance of official Government business, more specifically, in support of the FDIC and this TO.

#### **H.7.1.2.2 ASSIGNMENT OF ACCESS RIGHTS**

Access to FDIC IT resources shall be controlled and given only on a job-needed basis. Such access shall initially be approved by the FDIC OM and tracked to ensure proper usage and accountability.

#### **H.7.1.2.3 PHYSICAL ACCESS**

The contractor shall adhere to the physical access standards or procedure established by the FDIC. If physical access to a restricted premise or IT resource is required by contractor or subcontractor personnel, a process shall be put in place to verify that the access is properly justified and approved.

#### **H.7.1.2.4 LOGICAL ACCESS**

Contractor shall follow approved FDIC DIT Access Control processes before personnel acquire logical access to IT resources. Access to critical resources such as system files, logs and production data by personnel shall not be allowed unless such access is properly justified and approved by FDIC's OM (in advance). Access to restricted resources shall be regularly tracked, monitored and reviewed.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

### **H.7.1.2.5 REMOTE ACCESS**

Contractor, its employees and subcontractors shall follow FDIC remote access processes and procedures. Before obtaining such access, access requests must be reviewed and approved by both an FDIC authorizing official and the contract manager.

### **H.7.1.2.6 NETWORK ACCESS REQUIREMENTS**

The contractor shall comply with all provisions of FDIC Circular 1360.17, Information Technology Security Guidance for FDIC Information Technology Procurements/Third Party Products.

### **H.7.1.2.7 COMPLIANCE WITH THE ACCESS CONTROL REQUIREMENTS**

The contractor shall comply with the following:

- Access to FDIC Information Systems, 7.5.1-3 (PGI), (See Section H.7.1.8.7)

### **H.7.1.3 SECURITY TRAINING AND COMPETENCY**

The contractor shall assign the relevant skilled and experienced personnel to operate the FDIC services. The personnel shall be familiar with the requirements of the FDIC service and adhere to the FDIC security policy, standards, and procedures stipulated by the FDIC.

#### **H.7.1.3.1 SECURITY AWARENESS IN WORK AREA**

The contractor shall ensure that the assigned personnel are fully aware of the security needs and risks in his/her assigned areas of work. This gives assurance to the FDIC that these personnel will not, intentionally or unintentionally, compromise the security of the FDIC service.

#### **H.7.1.3.2 CONTRACTOR COMPLIANCE WITH THE SECURITY TRAINING AND COMPETENCY REQUIREMENTS**

The contractor shall be responsible for ensuring that all assigned contractor employees have received up-to-date IT Security Training, specific to the technology/platform they will be supporting at the FDIC, and that each contractor employee shall undergo refresher IT Security Training on at least an annual basis. The contractor shall be able to provide the FDIC with proof-of-training for each contractor employee. The FDIC reserves the right to assess the IT Security Training each contractor employee has taken (or will be taking) and to require alternative and/or additional training should the existing training content be deemed inadequate or irrelevant.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

The contractor shall ensure that its personnel designing, programming, operating, using, or managing FDIC systems/network and/or data in performance of the TO, are properly trained and must receive training at least annually in IT security awareness and security practices, policies, and procedures as required under the Computer Security Act of 1987 and OMB Circular A-130, including Appendix III. In addition, the contractor shall ensure that IT security training also meets the requirements stated in the NIST special publications and in the FDIC circulars referenced in this Article. The contractor shall certify on an annual basis that its personnel working on the contract have successfully completed all required IT security training and that they are aware of their IT security responsibilities.

All contractor and subcontractor employees being granted access to FDIC's network/systems must review the FDIC Security Awareness Website (located at [http://fdic01/division/dirm/itm\\_web/dirm\\_pages/infosec/secawareness/secawareness.htm](http://fdic01/division/dirm/itm_web/dirm_pages/infosec/secawareness/secawareness.htm)) and provide electronic certification of their review within five business days of receiving a network ID.

### **H.7.1.4 CONFIDENTIALITY OF INFORMATION, DATA, SYSTEMS**

The contractor must ensure the confidentiality of all information, data, and systems provided by FDIC or used or obtained by contractor personnel under this TO and prevent its inappropriate or unauthorized use or disclosure. The contractor and all employees working on an FDIC contract/TO must sign the contractor Confidentiality Agreement (FDIC form 3700-46 and/or FDIC form 3700-46A) (**See Section J, Attachment GGG**) no later than five business days after starting performance and prior to receiving such information, or when receiving their badges, and return the signed Agreements to the FDIC OM. This includes contractor personnel who are required to work on-site at an FDIC facility or have access to FDIC sensitive information or data, systems or network. Failure to provide the signed Agreements may result in the removal of the employee from performing under the contract.

Contracts required to design, develop, operate or maintain a system containing personal information to accomplish an FDIC function, must complete a Privacy Threshold Analysis to determine if the system contains personally identifiable information and is considered a system of records subject to the Privacy Act of 1974. The Privacy Act requires a Privacy Impact Assessment when developing or buying an information technology system that contains personal information about members of the public. If the FDIC program office confirms that the services being performed are subject to the Privacy Act, the name of the system of records and privacy and security requirements must be provided to the FDIC DIT ISPS Privacy section.

#### **H.7.1.4.1 COMPLIANCE WITH THE CONFIDENTIALITY OF INFORMATION, DATA, SYSTEMS REQUIREMENTS**

The contractor shall comply with the following:

- Privacy Act (JULY 2008), 7.5.1-1 (PGI), (See Section H.7.1.8.5)

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- Protecting Sensitive Information (SEPTEMBER 2010), 7.5.1-2 (PGI), (See Section H.7.1.8.6)
- Access to FDIC Information Systems, 7.5.1-3 (PGI), (See Section H.7.1.8.7)

### **H.7.1.5 SECURITY ROLES AND RESPONSIBILITIES**

The Contract personnel involved in the FDIC service shall be clearly defined and communicated. Clear definition of roles and responsibilities should not only ensure accountability and proper segregation of duty, but also prevent conflicting or duplicating roles from being defined.

### **H.7.1.6 INFORMATION HANDLING AND DISCLOSURE**

#### **H.7.1.6.1 CONFIDENTIALITY AGREEMENTS**

Personnel of the TO who are to work on the FDIC service are required to sign a confidentiality agreement to protect FDIC against unauthorized disclosures of confidential information accessed by the personnel in the course of their work.

#### **H.7.1.6.2 PROPER HANDLING OF CRITICAL INFORMATION**

The TO personnel, who need to handle or are in custody of sensitive or confidential information, shall follow the FDIC policies on handling and managing these information to ensure that the information is given the necessary protection.

#### **H.7.1.6.3 DISCLOSURE OF SECURITY INFORMATION**

The contractor shall put in place a process to protect FDIC against unauthorized disclosure of security information of the FDIC service, without the necessary approval or beyond the scope defined by the FDIC.

### **H.7.1.7 OUTSOURCED INFORMATION SERVICE PROVIDER**

An outsourced information service can be defined as a specific third-party information processing solution procured with the intent of leveraging existing technologies and processes which provide significant cost reduction over an outsourced or agency owned information system. Any one of the following must be true about an outsourced information service:

1. The outsourced information service uses proprietary technology to provide the same solution to multiple clients and, as a result, only a fraction of the technology components may be available for an agency's review (Software as a Service, "SaaS," "Cloud Computing," etc.)
2. The outsourced information service acts as a hosting provider for a COTS product whose application logic has not been altered.



## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

3. The outsourced information service does not receive data feeds from the agency and all data feeds are from outsourcer to agency. (This does not apply to user provided input or initial data-loads.)

The outsourced information service provides only pay-per-use CPU cycles (GRID computing, Symmetric multi-processing, etc.) without any application or transactional logic.

All outsource services that are purchased or renewed by the contract in behalf of FDIC shall:

1. Include the latest security and privacy provisions and clauses from the Mission Capability section of the Acquisitions Procedure, Guidance, and Information Guide into all FDIC solicitations.
2. Include the latest security and privacy provisions and clauses from the Acquisitions Procedures, Guidance, and Information Guide into statements of work and contract documents based on the prescription.
3. Outsourced Service Provider shall provide the FDIC with any security documentation as required by the FDIC ISPS division. This includes, but is not limited to, IT Security to IT Security Plan, Incident Response Plan, and any independent assessments prior to acquisition.
4. The outsource service PM shall complete Application Security Assessment (ASA), Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) Template for Outsourcers, Interconnection Security Agreement (ISA) / Memorandum of Agreement (MOA) and the eAuthentication Risk Assessment forms.
5. The above forms shall be processed by the Information Security Manager (ISM). Once the forms are approved the contract can purchase or renew the outsource service on behalf of FDIC.
6. Outsourced Information Service Provider Transitions. In the case of transitions from one outsourced information service provider to another, the division and outsourced information service provider(s) are required to document their detailed transition plans to mitigate potential security and privacy risks and ensure smooth transition.
7. Vendor Disposition. FDIC Data Disposal – Outsourced Information Service Providers shall sanitize all data upon termination of work for FDIC.
8. FDIC Data Retention. Data retention shall be conducted at the discretion of the Oversight Manager.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

9. Access Removal. At the termination of work for FDIC, the Oversight Manager must ensure that any access provided to the vendor has been removed. This includes access to the FDIC network and any offsite FDIC resources.

### **H.7.1.7.1 COMPLIANCE WITH THE OUTSOURCED INFORMATION SERVICE REQUIREMENTS**

The contractor shall comply with the following:

- a. Security and Privacy Compliance for IT Service (JULY 2008), 7.4.2-1 (PGI), (See Section H.7.1.8.1)
- b. Off-Site Processing & Storing of FDIC Information (JUNE 2010), 7.4.2-2 (PGI), (See Section H.7.1.8.2)
- c. Data Connection (JULY 2008), 7.4.2-3 (PGI), (See Section H.7.1.8.3)
- d. Security and Privacy Requirements for External Web Application and Content (JULY 2008), 7.4.2-4 (PGI), (See Section H.7.1.8.4)
- e. Privacy Act (JULY 2008), 7.5.1-1 (PGI), (See Section H.7.1.8.5)
- f. Protecting Sensitive Information (SEPTEMBER 2010), 7.5.1-1 (PGI), (See Section H.7.1.8.6)
- g. Access to FDIC Information Systems (June 2010), 7.5.1-3 (PGI), (See Section H.7.1.8.7)

### **H.7.1.8 FDIC SECURITY CLAUSES**

#### **H.7.1.8.1 SECURITY AND PRIVACY COMPLIANCE FOR IT SERVICES (JULY 2008), 7.4.2-1 (PGI)**

- a. Security and Privacy Compliance. The contractor is responsible for IT security for contractor Personnel and subcontractor personnel granted access to the FDIC network, and for their use of systems connected to the FDIC network, and for those systems developed, maintained, implemented or operated by the contractor for FDIC. All IT products and services provided by the contractor shall comply with all FDIC information security and privacy directives, policies and requirements unless contractor obtains a written waiver from FDIC Information Security/Privacy staff.
- b. Laws and Standards. All IT products and services provided by the contractor must comply with Federal laws and standards addressing information security. These include:
  1. The Privacy Act of 1974 (5 U.S.C. § 552a) as amended (if incorporated in the contract)
  2. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources (Transmittal Memorandum No. 4) including Appendices
  3. E-Government Act of 2002 (P. L. 107-347) including Title II, Section 208 - Privacy Provisions and Title III - Federal Information Security Management Act of 2002 (FISMA), and related OMB guidance

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

4. National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications
- c. FDIC Policy and Guidance. All IT products and services provided by the contractor shall address information security and privacy requirements throughout their design, development, implementation, maintenance, operation, and termination as provided in FDIC system development life cycle policy and guidance. This includes completing or providing the necessary information for the FDIC to complete privacy impact assessments, security assessments, risk assessments, security plans, contingency plans, and other security and privacy artifacts as required.
- d. Subcontracts. Contractor must include this clause in all its subcontracts to which the conditions and requirements described in this clause would apply. Contractor also must require its subcontractors (first-tier) to include this clause in any of their subcontracts (second-tier) to which the conditions and requirements of this clause would apply.

### **H.7.1.8.2 OFF-SITE PROCESSING & STORING OF FDIC INFORMATION (JUNE 2010), 7.4.2-2 (PGI)**

- a. Protection of Information. The Contractor shall implement adequate administrative, technical, physical, and procedural security controls to ensure that all FDIC information in its possession or under its control is adequately protected from loss, misuse, and unauthorized access or modification. The collection, use, transmission, and disclosure of FDIC information shall comply with all federal and state privacy laws and FDIC rules and regulations regarding privacy. The Contractor shall further ensure that FDIC PII is separated both physically and logically from Contractor's data. The Contractor shall not use any FDIC information except to the extent necessary to carry out its obligations under the contract. Contractor shall not disclose FDIC information to any third party unless disclosure is authorized in the contract or Contractor obtains the prior written consent of the Contracting Officer.
- b. Control of Information. All FDIC information remains the property of FDIC. At any time, upon request of the Contracting Officer, Contractor shall promptly retrieve and deliver to FDIC all FDIC information, or any portion of information as specified by FDIC, under the Contractor's control or in its possession. Information shall be provided in a format and on media as agreed by both parties. The Contractor shall not, and shall not permit any other person, to access, transmit, maintain, store, use or disclose the Confidential Information [Sensitive information] outside of the United States. Upon completion or termination of the contract, or at any time the Contracting Officer requests it in writing, Contractor shall return, erase, or destroy all FDIC information on any media under its control or in its possession, as FDIC directs.
- c. Security Plan. The Contractor shall implement and maintain the approved IT Security Plan, Physical/Environmental Security Plan, or the approved security audit or review, which is

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

hereby incorporated into the contract, for the duration of the contract. The Contractor must demonstrate its continued compliance with the controls, processes and procedures described in the Security Plan (or the security audit or review) throughout the term of the contract, as FDIC may request. If providing infrastructure support on a contractor site, the contractor shall provide their IT Security Plan (**See Section F, Deliverable 39**) for review by FDIC auditors, to ensure FDIC data and information remain secure.

- d. Inspections/Assessments. The Contractor shall allow and cooperate with both scheduled and unannounced inspections and assessments of its facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. Government Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis and throughout the term of the contract or TO, to ensure and verify compliance with FDIC IT security and privacy requirements.
- e. Monitoring and Incident Response. The Contractor shall monitor its facility and premises for security and privacy incidents and provide the capability to respond to and resolve them effectively and in a timely manner. All security and privacy incidents that involve FDIC information must be immediately reported to FDIC's Computer Security Incident Response Team (CSIRT).
- f. Contact Information. The Contractor shall provide a point of contact (name, telephone number, e-mail address) with whom the Contracting Officer, Oversight Manager, and FDIC Information Security and Privacy Staff may communicate throughout the duration of the contract about information security and privacy issues.

### **H.7.1.8.3 DATA CONNECTION (JULY 2008), 7.4.2-3 (PGI)**

- a. Pre-connection Requirements. Prior to the establishment of data connections, contractor shall allow and cooperate with FDIC to conduct physical review(s) of contractor premises and facilities. The contractor shall execute an Interconnection Security Agreement/Memorandum of Understanding with FDIC prior to establishing any data connection between the FDIC network and contractor facility.
- b. FDIC Network Segments. If the FDIC network is extended into the contractor's facility, the contractor shall connect only FDIC-provided or FDIC-approved hardware containing FDIC-provided software to that FDIC-network segment unless prior written waiver and approval of the FDIC Oversight Manager and FDIC information technology staff has been received. contractor-issued security patches shall be applied promptly to operating system and other software running on network-attached hardware. The contractor shall keep all FDIC network equipment located in contractor's facilities in a secured area with controlled access. The contractor, at all times, shall isolate all FDIC-network segments and associated equipment located at the contractor's facility from any non-FDIC networks located at the same facility. FDIC-network segments shall not be connected to non-FDIC network segments. Equipment

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

(desktops, laptops, printers, etc.) shall not be simultaneously connected to both FDIC and non-FDIC networks.

### **H.7.1.8.4 SECURITY AND PRIVACY REQUIREMENTS FOR EXTERNAL WEB APPLICATION AND CONTENT (JULY 2008), 7.4.2-4 (PGI)**

- a. The contractor shall ensure that each publicly accessible web site that is developed or maintained for FDIC under this contract conforms to the privacy requirements of the E-Government Act of 2002 (44 U.S.C. Ch. 36). The web site shall not use persistent cookies or other persistent tracking devices, unless FDIC approval for its use has been granted. Session cookies may be used on FDIC public-facing web sites. FDIC specific home pages and all major entry points into the website, and all web pages that collect personally identifiable information shall include a hyperlink labeled “Privacy Policy” that links to the FDIC’s privacy policy located on FDIC.gov. The web site also must accommodate additional forms of privacy notice, when deemed necessary by FDIC.
- b. The contractor shall provide access to FDIC for the purpose of performing scans or conducting other verification techniques to ensure the above requirements are met.

### **H.7.1.8.5 PRIVACY ACT (JULY 2008), 7.5.1-1 (PGI)**

- a. NOTICE. The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an FDIC function subject to the PRIVACY ACT OF 1974 (“THE ACT”), PUBLIC LAW 93-579, DECEMBER 31, 1974 (5 U.S.C. 552a) and applicable FDIC regulations. Violation of THE ACT may involve the imposition of criminal penalties.
- b. The Contractor agrees to:
  1. Comply with THE ACT and the FDIC rules and regulations issued under THE ACT in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:
    - (i) The systems of records; and
    - (ii) The design, development, or operation work that the contractor is to perform;
  2. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the design, development, or operation of a system of records on individuals that is subject to THE ACT; and

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

3. Include this clause - including this subparagraph (3) - in all subcontracts awarded under this contract which require the design, development, or operation of such a system of records.
- c. In the event of violations of THE ACT, a civil action may be brought against the FDIC when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an FDIC function, and criminal penalties may be imposed upon the officers or employees of the FDIC when the violation concerns the operation of a system of records on individuals to accomplish an FDIC function. For purposes of THE ACT, when the contract is for the operation of a system of records on individuals to accomplish an FDIC function, the Contractor and any employee of the Contractor is considered to be an employee of the FDIC.
- d. DEFINITIONS. As used in this clause:
  1. "Operation of a system of records" means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.
  2. "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.
  3. "System of records on individuals" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

### **H.7.1.8.6 PROTECTING SENSITIVE INFORMATION (SEPTEMBER 2010), 7.5.1-2 (PGI)**

- a. Sensitive Information Defined. Sensitive information is any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled. It includes the following:
  1. Information that is exempt from disclosure under the Freedom of Information Act, such as trade secrets and commercial or financial information, information compiled for law enforcement purposes, personnel and medical files, and information contained in bank examination reports;
  2. Information under the control of FDIC contained in a Privacy Act system of record that is retrieved using an individual's name or by other criteria that identifies an individual;

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

3. PII about individuals maintained by FDIC that if released for unauthorized use may result in financial or personal damage to the individual to whom such information relates. Sensitive PII, a subset of PII, may be comprised of a single item of information (e.g., SSN) or a combination of two or more items (e.g., full name along with, financial, medical, criminal, or employment information). Sensitive PII presents the highest risk of being misused for identity theft or fraud; and
  4. Information about insurance assessments, resolution and receivership activities, as well as enforcement, legal, and contracting activities; and
  5. Information related to information technology specific to the FDIC that could be misused by malicious entities (e.g., internal IP addresses, server names, firewall rules, encryption and authentication mechanisms, and network architecture pertaining to FDIC).
- b. Protecting Sensitive Information. Contractor, all contractor Personnel, subcontractors and subcontractor personnel shall comply with FDIC Circular 1360.9, Protecting Sensitive Information, and protect the confidentiality, integrity and availability of sensitive information, including personally identifiable information (PII), to which they have access. FDIC Circular 1360.9 is available at the FDIC website:  
[www.fdic.gov/buying/goods/acquisition/index.html](http://www.fdic.gov/buying/goods/acquisition/index.html).
- c. Controlling Sensitive Information. All sensitive information, electronic and paper copy, remains the property of FDIC. Sensitive information shall not be moved outside of FDIC premises or networks/systems unless this contract contains clause 7.4.2-2, Off-site Processing and Storing of FDIC Information.
- d. Confidentiality Agreement. An authorized representative of the Contractor, its subcontractors and consultants, and all personnel (key personnel and non-key personnel) who will have access to FDIC facilities, networks and/or information systems, or sensitive information (whether in hardcopy or electronic form) must execute confidentiality agreements. FDIC Form 3700/46, Confidentiality Agreement (for Contractors/Subcontractors/Consultants) and FDIC Form 3700/46A, Confidentiality Agreement (for Contractor/Subcontractor/Consultant Personnel) are included as attachments to this contract. The 3700/46 forms must be signed by the Contractor, and each subcontractor or consultant and submitted at the time of award to the Contracting Officer, with the signed contract. Post-award, they must be submitted to the Contracting Officer when a new subcontractor or consultant is being requested. FDIC Form 3700/46, Confidentiality Agreement (for contractor) and FDIC Form 3700/46A, Confidentiality Agreement (for contractor Personnel) are included as attachments to this contract. The 3700/46A forms executed by personnel must be submitted to FDIC no later than five (5) business days after starting performance and prior to receiving any sensitive information. The Contractor must submit the 3700/46A forms signed by key personnel to the Contracting Officer and those signed by non-key personnel to the Oversight Manager. Key personnel and

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

non-key personnel who are required to sign a confidentiality agreement, and do not sign, will not be permitted to perform work on the contract.

- e. Information Security and Privacy Awareness Training. Any key personnel or non-key personnel with access to sensitive information, who do not have access to the FDIC network and therefore are unable to take FDIC's on-line Information Security and Privacy Awareness Training, must obtain from the Oversight Manager a copy of FDIC's Information Security and Privacy Awareness Training on a CD or DVD. Upon completion of the training, they must provide confirmation via email to the Oversight Manager. The email must contain the following:

- trainee's name and phone number;
- contract number;
- name of the Contractor (and subcontractor or consultant, if applicable), and
- date the training was completed.

The training and email confirmation to the Oversight Manager must be accomplished prior to the individual's initial receipt of any sensitive information, and annually thereafter until contract performance is completed. Contractor must keep a record of when the training was accomplished, and provide it to FDIC upon request. Failure to complete this training and provide email confirmations within the required timeframes may result in removal from the task order.

- f. Subcontracts. Contractor must include this clause in all its subcontracts to which the conditions and requirements described in this clause would apply. Contractor also must require its subcontractors (first-tier) to include this clause in any of their subcontracts (second-tier, third-tier, etc.) to which the conditions and requirements of this clause would apply.

### **H.7.1.8.7 ACCESS TO FDIC INFORMATION SYSTEMS (JUNE 2010), 7.5.1-3 (PGI)**

- a. Contractor, all Contractor Personnel, subcontractors and subcontractor personnel granted access to FDIC's network/systems must comply with these FDIC directives:
1. Information Security and Privacy Awareness Training. FDIC Circular 1360.16 *Mandatory Information Security Awareness Training*, which requires the completion of on-line FDIC- information security and privacy awareness training and electronic certification of completion within five (5) business days of receiving an FDIC network ID, and annually thereafter until such time as the access is terminated. Failure to complete this training and provide electronic certification within the required timeframes will result in revocation of network/system access privileges and possible removal of contractor personnel from the contract.



## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

2. Acceptable Use of Information Technology Resources. FDIC Circular 1300.4 *Acceptable Use Policy for Information Technology Resources*, which outlines the permitted and prohibited uses of FDIC hardware, software, and information technology services.
  3. Passwords. FDIC Circular 1360.10 *Corporate Password Standards* for password configuration and maintenance requirements, which requires the use of strong passwords, changing passwords at prescribed intervals and the protection of passwords.
  4. Access Control. FDIC Circular 1360.15 *Access Control for Information Technology Resources*, which governs the granting and revocation of access to information technology resources, including the initial approval, continued review, and eventual termination of access. Contractor shall promptly notify Oversight Manager and Contracting Officer when personnel join or leave the contract so access may be granted or revoked without delay.
  5. Reporting Security Incidents. FDIC Circular 1360.12 *Reporting Computer Security Incidents*, which requires reporting to FDIC's Computer Security Incident Response Team (CSIRT) of all suspected or actual security or privacy incidents involving unauthorized access, misuse, tampering, bypassing security controls, alteration, disclosure or theft of information technology resources, data, and passwords .
- b. Subcontracts. Contractor must include this clause in all its subcontracts to which the conditions and requirements described in this clause would apply. Contractor also must require its subcontractors (first-tier) to include this clause in any of their subcontracts (second-tier) to which the conditions and requirements of this clause would apply.
- c. The FDIC Circulars identified in this clause are available on the FDIC website: [www.fdic.gov/buying/goods/acquisition/index.html](http://www.fdic.gov/buying/goods/acquisition/index.html)

### **H.7.1.8.8 IDENTIFICATION/ACCESS BADGES (JULY 2008). 7.5.2-11 (PGI)**

All contractor and subcontractor employees regularly working on-site at an FDIC facility must be issued an identification/access control badge. Such employees will not be granted on-site access until receiving the badge. Renewal of the badges is required semiannually.

### **H.7.1.8.9 USE OF FDIC PREMISES BY CONTRACTOR PERSONNEL (JULY 2008). 7.5.2-13 (PGI)**

Contractor shall comply with the FDIC directives governing access to and operations at FDIC offices and facilities, while on FDIC premises. The directives are available at the FDIC website: [www.fdic.gov/buying/goods/acquisition/index.html](http://www.fdic.gov/buying/goods/acquisition/index.html), or may be obtained from the Oversight Manager. Contractor is responsible for assuring that its personnel understand and observe these

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

directives. Contractor shall perform its contract activities in a manner which does not interrupt or interfere with the business conducted at FDIC.

Subcontracts. Contractor must include this clause in all its subcontracts to which the conditions and requirements described in this clause would apply. Contractor also must require its subcontractors (first-tier) to include this clause in any of their subcontracts (second-tier) to which the conditions and requirements of this clause would apply.

### **H.7.1.8.10     TITLE 12, CFR, PART 366**

All contractors that perform work for the FDIC are required to be in compliance with the requirements of Title 12, CFR, Part 366. This integrity and fitness process requires the completion and submission of the following administrative forms: 1.) FDIC contractor Representations and Certifications; 2.) FDIC Integrity and Fitness Representations and Certifications; 3.) Background Investigation Questionnaire For contractors; 4.) Background Investigation Questionnaire For contractor Personnel and Subcontractors and 5.) Notice and Authorization Pertaining to the Fair Credit Reporting Act of 1970, 15 U.S.C, Section 1681, et. seq.

### **H.7.1.8.11     BACKGROUND INVESTIGATION QUESTIONNAIRES, (JULY 2008), 7.5.2-1 (PGI)**

Offeror shall submit the following document, signed by an authorized representative:

- Background Investigation Questionnaire for Contractors (FDIC 1600/7) (Attachment YY).

The offeror shall submit the document entitled “Background Investigation Questionnaire for Contractors” (FDIC 1600/7) (Attachment YY) in a sealed envelope with its written technical proposal. The information submitted on these forms must be accurate to the best of the offeror’s knowledge and complete so as not to delay the investigation and evaluation process.

In addition, offeror shall submit the following documents, completed and signed by all Key Personnel the FDIC OM (G.3.5.1) two days after TOA. After this milestone the contractor shall submit the following documents for all personnel (prime and sub) to include key personnel substitutions.

- Background Investigation Questionnaire for Contract Personnel and Subcontractors (FDIC 1600/4) (Attachment AAA);
- Notice and Authorization Pertaining to Consumer Reports (FDIC 1600/10) (Attachment XX);
- Questionnaire for Public Trust Positions (SF 85P) (Section J, Attachment VVV);
- Personnel Security Action Request (FDIC 1600/13) (Section J, Attachment WWW);

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

- Employee/Contractor Identification Card Request (1620/01) (Section J, Attachment XXX); and,
- Declaration of Federal Employment, Submission Requirements for Contractor Personnel (Optional Form (OF)-306) (Section J, Attachment YYY)
- Additional Background Security Questions for Contractor Personnel (FDIC 1600/25) (Section J, Attachment ZZZ)

The information submitted on these forms must be accurate to the best of the offeror's knowledge and complete so as not to delay the investigation and evaluation process.

The offeror must also comply with additional background investigation requirements, as set forth in clause 7.5.2-3, Background Investigations.

### **H.7.1.8.12 BACKGROUND INVESTIGATIONS, ALTERNATE 1 (May 2009), 7.5.2-3 (PGI)**

Substitute the following paragraph (a) for paragraph (a) of the basic clause 7.5.2-3.

a. Any Contractor Personnel or subcontractor personnel who:

- work on-site at and have unescorted access to FDIC offices or facilities, or
- have access to FDIC networks/systems

must undergo a background investigation, in accordance with FDIC Circular 1610.2. In addition, background investigations are conducted on all:

- Contractor Personnel on contracts and other awards for services with a value greater than \$100,000, and
- subcontractor personnel on subcontracts for services with a value greater than \$100,000.

Background investigations may be done on any contract or award at the discretion of the FDIC. The extent of the background investigation conducted will be in direct relation to the risk level assigned either in clause 7.5.2-9, *Risk Level Designation – Entire Contract* or in clause 7.5.2-10, *Risk Level Designation – Labor Category*. FDIC Circular 1610.2 is available at the FDIC website: [www.fdic.gov/buying/goods/acquisition/index.html](http://www.fdic.gov/buying/goods/acquisition/index.html)

### **H.7.1.8.13 FDIC CIRCULAR 1610.2, PERSONNEL SECURITY POLICY AND PROCEDURES FOR FDIC CONTRACTORS**

The integrity and fitness requirements apply to all contractors seeking to perform services on behalf of the FDIC. In addition, all contractor personnel who will have long term access to FDIC facilities, sensitive information, or Information Technology Resources, must meet minimum security standards required by regulation. This policy shall not apply to intermittent vendors who access FDIC facilities on an infrequent and generally unscheduled basis, and do not

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

require access to sensitive information (i.e., equipment repair, delivery personnel, etc.). These vendors should not be processed under this circular, but must be continuously and attentively escorted, kept under visual surveillance, and work only during normal business hours. Building maintenance, repair and custodial workers may require security checks consisting of fingerprint checks to allow unescorted access to FDIC space.

Provisions of this policy may be waived based on the operational needs of the FDIC and upon the request of an FDIC Division Director and the concurrence of the Associate Director, Corporate Services Branch.

### **H.9 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS**

#### **H.9.1 ORGANIZATIONAL CONFLICT OF INTEREST**

If the contractor has or is currently providing support or anticipates providing support to Federal Deposit Insurance Corporation (FDIC) that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI in accordance with FAR Subpart 9.5. The contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the contractor (and any subcontractors, consultants, or teaming partners) agrees to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be identified and addressed in accordance with FAR Subpart 9.5.

**Such requirements are in addition to those specified in 12 CFR Part 366; in the event of a conflict between this provision and the requirements of 12 CFR Part 366, the latter shall control.**

#### **H.9.2 NON-DISCLOSURE REQUIREMENTS**

If the contractor acts on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (Section J, (insert Attachment reference)) and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

- a. Are listed on a signed Addendum to Corporate Non-Disclosure Agreement (NDA) Form (**Section J, Attachment HHH**) prior to the commencement of any work on the TO.
- b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.
- c. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel also must be listed on a signed Addendum to Corporate NDA and be instructed in the requirements of FAR 3.104. Any information provided

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

### **H.14 SECTION 508 COMPLIANCE REQUIREMENTS**

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., contractor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

### **H.16 COST ACCOUNTING SYSTEM**

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS), affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and contract performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the contract.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

### **H.18      PURCHASING SYSTEMS**

The possession of an approved contractor purchasing system is to further the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting.

With the original proposal submission and prior to the award of a TO the CO shall verify the possession of the contractor's approved purchasing system. Thereafter, the contractor is required to certify to the CO no later than 30 calendar days prior to the exercise of any options the continued possession and approval of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the CO within ten workdays from the date the results are known to the contractor.

### **H.23      TRAVEL**

#### **H.23.1    TRAVEL REGULATIONS**

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- a. Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
- b. Joint Travel Regulations (JTR), Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.

#### **H.23.2    TRAVEL AUTHORIZATION REQUESTS**

Before undertaking travel to any Government site or any other site in performance of this Contract, the contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name and destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the contractor shall prepare a Travel Authorization Request for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR.

Requests for travel approval shall:

- a. Be prepared in a legible manner.
- b. Include a description of the travel proposed including a statement as to purpose.
- c. Be summarized by traveler.
- d. Identify the TO number.
- e. Identify the CLIN and Interagency Agreement account associated with the travel.
- f. Be submitted in advance of the travel with sufficient time to permit review and approval.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

### **H.24 ANCILLARY PRODUCTS AND SERVICES**

The Contractor may be required to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified after award. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the FEDSIM COR a Request to Initiate Purchase (RIP). The RIP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the COR without complying with the requirements of **Section H.25**, Commercial Software Agreements.

### **H.25 COMMERCIAL SOFTWARE AGREEMENTS**

H.25.1 The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in **Section H.24** and as contemplated in the Ancillary Products and Services CLINs in **Section B.7** may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as "clickwrap" or "browsewrap" (collectively, "software agreements"). The parties acknowledge that the FAR clause at 12.212(a) requires the Government to procure such tools and their associated documentation under such Software Agreements to the extent such Software Agreements are consistent with Federal law.

H.25.2 In order to ensure that the software agreements are consistent with Federal law, the contractor shall not make any purchase contemplated in **Section H.24** above without first securing the consent of the licensor of such software tools to amend the software agreements in accordance with the Amendment clause set forth in **Section H.25.4** below. The contractor shall submit documentary evidence of such consent before any final RIP/CTP approval, as identified in **H.24** above, will be provided by the Government.

H.25.3 The requirements of this **Section H.25** apply only to those commercial software tools newly purchased under this TO; they do not apply to software furnished as GFI/GFE (if any). Further, they apply only to those software agreements that define the Government as the licensee or are intended to be transferred or assigned to the Government, with the Government becoming the licensee, at the end of this TO.

H.25.4 As used in the Amendment clause, the term "this Agreement" refers to each Software Agreement. The relevant definitions and the capitalization of terms (e.g., licensee, licensor, software agreement) may be adjusted as necessary to match the nomenclature of the Software Agreement.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

### **Amendment**

For Federal Government Licensees, this Agreement is hereby amended as follows:

- a. Dispute resolution and governing law: Any arbitration, mediation, or similar dispute resolution provision in this Agreement is hereby deleted. This Agreement shall be governed by and interpreted and enforced in accordance with the laws of the United States of America, and dispute resolution shall take place in a forum, and within the time period, prescribed by applicable federal law. To the extent permitted by federal law and then only to the extent not pre-empted by federal law, the laws of the state specified in this Agreement (excluding its choice of law rules) will apply. No equitable or injunctive relief, and no shifting of legal fees or costs, may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
- b. Indemnification: Any provisions in this Agreement requiring any Federal Government Licensee to indemnify any party are hereby deleted and shall not apply. Any provisions requiring the licensor to indemnify the Federal Government Licensee shall be revised to state that such indemnification, and the conduct and/or settlement of any applicable proceedings, shall be subject to 28 USC 516.
- c. Changes in templates: This Agreement shall apply in the version attached hereto. Subsequent updates to or changes in the licensor's standard commercial templates for such agreements shall not be binding on the Federal Government Licensee, except by prior express written agreement of both parties.
- d. Fees, taxes and payment: If the Software is licensed as part of a separate Government contract between the Federal Government Licensee and a prime contractor, the provisions of such contract regarding fees, taxes and payment shall supersede any provisions of this Agreement regarding same. Notwithstanding the foregoing: (a) express written agreement of the Federal Government Licensee shall be required prior to (i) any extension or renewal of this Agreement or the associated fees or (ii) any change in the fees; (b) late payments shall be governed by the Prompt Payment Act and the regulations at 5 CFR 1315; and (c) no cost of collection on delinquent invoices may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
- e. Assignment: Licensor may not assign this Agreement or its rights or obligations there under, in whole or in part, except in accordance with the procedures set forth in FAR subparts 32.8 and/or 42.12, as applicable.
- f. No waiver of liability or cause of action: Any provision requiring the Federal Government Licensee to agree to waive or otherwise not to pursue any claim against the licensor it may otherwise have is hereby deleted. Without limiting the generality of the foregoing, the parties agree that nothing in this Agreement, including but not limited to the limitation of liability clauses, in any way grants the licensor a waiver from, release of, or limitation of



## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

liability pertaining to, any past, current or future violation of federal law and that no clause restricting users' statements shall be read to restrict the Federal Government Licensee's ability to pursue any course of action otherwise permitted by federal law, regulation, or policy, including without limitation making public statements in connection with any suspension or debarment action.

- g. Audit: Any clauses in this Agreement allowing for an audit of the Federal Government Licensee's records or information systems, or verification of its compliance with this Agreement generally, shall be subject to the Federal Government Licensee's requirements pertaining to security matters, including without limitation clearances to be held and non-disclosure agreements to be executed by auditors, badging or escorting requirements for access to premises, and other applicable requirements. Any over-use identified in an audit shall be referred to the prime contractor or the Federal Government Licensee's contracting officer (as applicable) for action. No audit costs may be sought against the Federal Government Licensee except as, and then only to the extent, specifically authorized by applicable federal statute.
- h. Compliance with laws: The parties acknowledge that the United States, as a sovereign, is subject to the laws of the United States. Nothing in this Agreement shall be interpreted to imply consent by any Federal Government Licensee to submit to the adjudicative or enforcement power of any regulatory, administrative, or judicial authority of, or the application of the laws of, another jurisdiction. Any provision inconsistent with applicable federal law that is not listed above is hereby deemed omitted from this Agreement to the extent of such inconsistency.
- i. Third party terms: Any third party licensing terms associated with third-party software components or products embedded in or otherwise provided with the software shall be deemed amended in accordance with **Sections a-h** above.

### **H.26      AWARD FEE**

See the Award Fee Determination Plan in Section J.

#### **H.26.1      ESTABLISHMENT AND DETERMINATION OF AWARD FEE**

The award fee dollar pool will be established on execution of the TO. The Government reserves the right to adjust these amounts to reflect any change in the Estimated Cost for award fee period. The amount of Award Fee is established at award and cannot exceed 8.9% award fee over the life of the order.

The Government AFDO will, at the conclusion of each specified evaluation period(s), evaluate the contractor's performance for a determination of award fee earned. The determination of the award fee amount and the methodology for determining the award fee are unilateral decisions made solely at the discretion of the Government.

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

The evaluation of contractor performance will be in accordance with the Award Fee Determination Plan (AFDP) (**Section H.26.2**). The Government will promptly advise the contractor in writing of the determination and reasons why the award fee was not earned. The contractor shall submit a self-evaluation of performance for each period under consideration. While it is recognized that the basis for the determination of the fee will be the evaluation by the Government, any self-evaluation which is received within 15 workdays after the end of the period being evaluated may be given consideration as deemed appropriate by the Award Fee Evaluation Board (AFEB). Any cost associated with the development and presentation of a self-evaluation will not be allowed as a direct cost to this TO.

### **H.26.2 AWARD FEE DETERMINATION PLAN (AFDP)**

An AFDP will be established by the Government, in consultation with the contractor, based on the objectives and concerns provided in the TOR and the contractor-provided solutions. The AFDP will include the criteria used to evaluate each area and the percentage of award fee available for each area. A separate Quality Assurance Surveillance Plan (QASP) will not be provided for this order as the AFDP will serve the purpose of the QASP.

The AFDP may be revised unilaterally by the Government at any time during the period of performance. The Government will make every attempt to provide changes to the contractor 15 workdays prior to the start of the evaluation period to which the change will apply. The AFDP may be re-evaluated each evaluation period with input from the contractor.

The Government may, at its option, unilaterally revise the plan to include metrics gathered from the re-evaluation to be applied in future award fee periods.

### **H.26.3 DISTRIBUTION OF AWARD FEE**

The Award Fee will be distributed in accordance with the AFDO determination and the AFDP (Section J).

If the Government initiates any action that impacts the contractual scope of work and/or schedule pursuant to the “changes” clause or other pertinent provisions of the TO, the maximum award fee available for payment for any evaluation periods impacted will be modified as negotiated between the parties.

### **H.28 INTELLECTUAL PROPERTY RIGHTS**

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply. The Software Agreements referenced in **Section H.25**, amended as contemplated therein, shall be deemed to constitute such disclosure with regard to their associated commercial software tools

## **SECTION H – SPECIAL CONTRACT REQUIREMENTS**

and shall prevail over any inconsistent provision in FAR 52.227-14 to the extent of such inconsistency.

### **H.29 LIMITATION ON ANCILLARY PRODUCTS AND SERVICES FIXED FEE**

The fixed fee to be applied to any Ancillary Products and Services acquisitions will be capped at the awarded fixed fee percentage based upon the Government agreed upon firm fix price (FFP) or not to exceed (NTE) costs (if T&M or Cost Type order) at time of Ancillary Product/Service "Request to Initiate Purchase" (RIP) Government approval. In the event actual costs are below the RIP approved stated FFP or NTE pricing, the Government will pay fixed fee based upon the lower value of actual costs incurred. In the event actual costs exceed the agreed upon NTE or FFP pricing at time of purchase order award, the Government will pay fixed fee only based upon the previously approved lower RIP NTE costs or FFP. In no event will the contractor be entitled to fixed fee that is not directly associated with a Government approved RIP, regardless of the amount of funding provided under the Ancillary Products and Services CLIN. The amount of costs, material handling, and fixed fee paid in total cannot exceed the total NTE Ancillary Products and Services CLIN ceiling (subject to funding) established for each applicable task order period.

## **SECTION I – CONTRACT CLAUSES**

### **I.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request the CO will make their full text available. Also, the full text of a provision may be accessed electronically at:

FAR website: <https://www.acquisition.gov/far/>

<b>Clause No</b>	<b>Clause Title</b>	<b>Date</b>
52.202-1	Definitions	(Jan 2012)
52.203-3	Gratuities	(Apr 1984)
52.203-5	Covenant Against Contingent Fees	(Apr 1984)
52.203-6	Restrictions on Subcontractors Sales to the Government	(Sept 2006)
52.203-7	Anti-Kickback Procedures	(Oct 2010)
52.203-8	Cancellation, Recession, and Recovery of Recovery of Funds for Illegal or Improper Activity	(Jan 1997)
52.203-10	Price of Fee Adjustment For Illegal or Improper Activity	(Jan 1997)
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	(Oct 2010)
52.203-13	Contractor Code of Business Ethics and Conduct	(Apr 2010)
52.203-14	Display of Hotline Posters: (3) link will be provided at time of award.	(Dec 2007)
52.204-2	Security Requirements	(Aug 1996)
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	(May 2011)
52.204-7	Central Contractor Registration	(Feb 2012)
52.204-9	Personal Identity Verification of Contractor Personnel	(Jan 2011)
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	(Aug 2012)
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	(Dec 2010)
52.215-2	<u>AUDIT AND RECORDS – NEGOTIATION</u>	(Oct 2010)
52.215-10	Price Reduction for Defective Certified Cost or Pricing Data	(Aug 2011)
52.215-11	Price Reduction for Defective Certified Cost or Pricing Data—Modifications	(Aug 2011)
52.215-12	Subcontractor Certified Cost or Pricing Data	(Oct 2010)
52.215-13	Subcontractor Certified Cost or Pricing Data—Modifications	(Oct 2010)
52.215-15	Pension Adjustments and Asset Reversions	(Oct 2010)
52.215-16	Facilities Capital Cost of Money	(Jun 2003)
52.215-17	Wavier of Facilities Capital Cost of Money	(Oct 1997)
52.215-18	Reversion of Adjustment of Plans for Postretirement Benefits (PRB) other Pensions	(Jul 2005)

## **SECTION I – CONTRACT CLAUSES**

<b>Clause No</b>	<b>Clause Title</b>	<b>Date</b>
52.215-21	Requirements for Cost or Pricing Data or Information Other than Cost or Pricing Data – Modifications	(Oct 2010)
52.215-21	<u>ALTERNATE I</u>	(Oct 2010)
52.216-7	<u>ALLOWABLE COST AND PAYMENT: A(3): 30<sup>TH</sup></u>	(Jun 2011)
52.217-8	Option to Extend Services Fill-In Date: no later than 60 days of contract expiration	(Nov 1999)
52.219-8	Utilization of Small Business Concerns	(Jan 2011)
52.222-2	Payment for Overtime Premiums: (a) Time and one half for non-salaried employees.	(Jul 1990)
52.222-3	Convict Labor	(Jun 2003)
52.222-21	Prohibition of Segregated Facilities	(Feb 1999)
52.222-26	Equal Opportunity	(Mar 2007)
52.222-35	Equal Opportunity for Veterans	(Sep 2010)
52.222-36	Affirmative Action for Workers with Disabilities	(Oct 2010)
52.222-37	Employment Reports Veterans	(Sep 2010)
52.222-50	<u>COMBATING TRAFFICKING IN PERSONS</u>	(Feb 2009)
52.222-54	<u>EMPLOYMENT ELIGIBILITY VERIFICATION</u>	(Jul 2012)
52.223-3	<u>HAZARDOUS MATERIAL IDENTIFICATION AND MATERIAL AND MATERIAL SAFETY DATA: (B) NONE</u>	(Jan 1997)
52.223-3	<u>ALTERNATE I</u>	(Jul 1995)
52.223-5	<u>POLLUTION PREVENTION AND RIGHT-TO-KNOW INFORMATION</u>	(May 2011)
52.223-5	Alternate I	(May 2011)
52.223-5	Alternate II	(May 2011)
52.223-6	Drug-Free Workplace	(May 2001)
52.223-10	Waste Reduction Program	(May 2011)
52.223-12	Refrigeration Equipment and Air Conditioners	(May 1995)
52.223-15	Energy Efficiency in Energy-Consuming Products	(Dec 2007)
52.223-16	IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products	(Sep 2007)
52.223-16	Alternate I	(Dec 2007)
52.224-1	Privacy Act Notification	(Apr 1984)
52.224-2	Privacy Act	(Apr 1984)
52.225-5	Trade Agreements	(Nov 2012)
52.225-8	Duty Free Entry	(Oct 2010)
52.225-13	Restrictions on Certain Foreign Purchases	(Jun 2008)
52.227-14	Rights in Data – General	(Dec 2007)
52.227-14	Alternate II	(Dec 2007)
52.230-2	Cost Accounting Standards	(May 2012)
52.230-3	Disclosure and Consistency of Cost Accounting Practices	(May 2012)
52.230-6	Administration of Cost Accounting Standards	(Jun 2010)
52.232-9	Limitation on Withholding of Payments	(Apr 1984)

Contract Number GS00Q09BGD0025

Task Order GST0013AJ0084

Modification PO12

## **SECTION I – CONTRACT CLAUSES**

<b>Clause No</b>	<b>Clause Title</b>	<b>Date</b>
52.232-20	Limitation of Cost	(Apr 1984)
52.232-22	Limitation of Funds	(Apr 1984)
52.232-23	Assignment of Claims	(Jan 1986)
52.232-23	Alternate I	(Apr 1984)
52.232-33	Payment By Electronic Funds Transfer – Central Contractor Registration	(Oct 2003)
52.233-1	Disputes	(Jul 2002)
52.233-1	Alternate I	(Dec 1991)
52.233-3	Protest After Award	(Aug 1996)
52.233-3	Alternate I	(Jun 1985)
52.233-4	Applicable Law For Breach of Contract Claim	(Oct 2004)
52.237-2	Protection of Government Buildings, Equipment, and Vegetation	(Apr 1984)
52.237-3	Continuity of Services	(Jan 1991)
52.237-10	Identification of Uncompensated Overtime	(Oct 1997)
52.239-1	Privacy or Security Safeguards	(Aug 1996)
52.242-1	Notice of Intent to Disallow Costs	(Apr 1984)
52.242-3	Penalties for Unallowable Costs	(May 2001)
52.242-4	Certification of Final Indirect Costs	(Jan 1997)
52.242-13	Bankruptcy	(Jul 1995)
52.243-2	Changes – Cost Reimbursement	(Aug 1987)
52.243-2	Alternate II	(Apr 1984)
52.243-7	Notification of Changes: <u>(b) 15 days</u>	(Apr 1984)
52.244-2	Subcontracts (d): Not applicable	(Oct 2012)
	Removed	
52.244-5	Competition in Subcontracting	(Dec 1996)
52.244-6	Subcontracts for Commercial Items	(Dec 2010)
	Removed	
52.245-1	Government Property	(Apr 2012)
52.245-9	Use and Charges	(Apr 2012)
52.246-23	LIMITATION OF LIABILITY	(Feb 1997)
52.246-25	Limitation of Liability – Services	(Feb 1997)
52.247-14	Contractor Responsibility for Receipt of Shipment	(Apr 1984)
52.247-67	Submission of Transportation Documents for Audit: <u>(c) COR</u> – See Section G	(Feb 2006)
52.249-6	Termination (COST-REIMBURSEMENT)	(May 2004)
52.249-14	Excusable Delays	(Apr 1984)
52.251-1	Government Supply Sources	(Aug 2012)
52.251-2	Interagency Fleet Management System Vehicles and Related Services	(Jan 1991)
52.253-1	Computer Generated Forms	(Jan 1991)

## **SECTION I – CONTRACT CLAUSES**

### **52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)**

- a. The Government may extend the term of this contract by written notice to the contractor within 30 days; provided that the Government gives the contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.
- b. If the Government exercises this option, the extended contract shall be considered to include this option clause.
- c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 4 years and six months.

(End of clause)

### **I.2 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), INCORPORATED BY REFERENCE**

The full text of a provision may be accessed electronically at:

GSAM website: <https://www.acquisition.gov/gsam/gsam.html>

<b>Clause No</b>	<b>Clause Title</b>	<b>Date</b>
552.232.25	Prompt Payment	(Nov 2009)

(End of Clause)

## **SECTION J – LIST OF ATTACHMENTS**

### **J.1 LIST OF ATTACHMENTS**

<b>Attachment</b>	<b>Title</b>
A	COR Designation Letter
B	Governance Requirements
C	Award Fee Plan Rev 5 dated 11.17.2014
D	Service Level Metrics
E	Draft FDIC Business Technology Strategic Plan 2013-2017
F	Service Locations
G	Reporting Requirements
H	End-User Computing Devices
I	Communications Systems
J	Telephony Equipment Profile
K	Printer and Multi-Function Devices
L	IT Server Inventory
M	Security Systems
N	Master Application List
O	Operating Systems- Servers
P	Commercial Off-The-Shelf Software
Q	Workstation Image Definition
R	Infrastructure Tooling- Deployed
S	Service Volumes
T	Current Asset Management System Profile
U	Current Incident Management System Profile
V	IOS Images
W	FDIC Change Management Process
W-1	FDIC Change Management Guide



## **SECTION J – LIST OF ATTACHMENTS**

<b>Attachment</b>	<b>Title</b>
W-2	ISC Change and Configuration Management Plan
W-3	Remedy Architecture Drawing
W-4	DIT-Wide Pre-approved Change List
X	Hardware & Software Maintenance Profile
Y	Mainframe Equipment and Lease
Z	Fulcrum Inventory
AA	ISB-ISC Services Catalog
BB	Workstation Image Build Modules
CC	Software on the Mainframe
DD	ITAS Applications
EE	Emergency Change Request Steps
FF	Manassas Inventory with Equipment Type
GG	ISC2_Call Volume Data
HH	Comparative Statistics_ISC 2
II	Data Center Statistics_ISC 2
JJ	Asset Management Data
KK	Video Teleconferencing Capability by City
LL	Severity 1 Notification and Escalation Process
MM	Regional Site Equipment List
NN	Typical Regional Site Racks
OO	Attachment Deleted
PP	Acronym List
QQ	Attachment Deleted
RR	Attachment Deleted
SS	Attachment Deleted
TT	Attachment Deleted

Contract Number GS00Q09BGD0025  
Task Order GST0013AJ0084  
Modification PO12

## **SECTION J – LIST OF ATTACHMENTS**

<b>Attachment</b>	<b>Title</b>
UU	Attachment Deleted
VV	Attachment Deleted
WW	FDIC Contractor Representations and Certifications
XX	Notice and Authorization Pertaining to Consumer Reports
YY	Background Investigation Questionnaire for Contractors (FDIC 1600/07)
ZZ	FDIC Integrity and Fitness Representations and Certifications (FDIC 1600/10)
AAA	Background Investigation Questionnaire for Contractor Personnel and Subcontractors (FDIC 1600/04)
BBB	FDIC IT Vision Document
CCC	FDIC Current Projects
DDD	Maintenance Roster
EEE	VIPs by Location
FFF	Problem Notification Report
GGG	FDIC Confidentiality Agreement (3700-46/3700-46A) - Updated
HHH	Employee/contractor Non-Disclosure Agreement (NDA)
III	Numbers of Users by City
JJJ	Help Desk Floor Plan
KKK	Floor Plan
LLL	DESS Oracle Middleware Support Historical Statistics
MMM	EMS Reference – Update Mod 10
NNN	ETS Reference – Update Mod 10
OOO	CSS Reference – Update Mod 10
PPP	PAS Reference
QQQ	EODS Reference
RRR	Dev, QA/Testing Support Reference
SSS	AAS Reference – Update Mod 10

## **SECTION J – LIST OF ATTACHMENTS**

<b>Attachment</b>	<b>Title</b>
TTT-B	Attachment Deleted
TTT-1	Attachment Deleted
TTT-2	Attachment Deleted
TTT-3	Attachment Deleted
TTT-4	Attachment Deleted
UUU	Attachment Deleted
VVV	Questionnaire for Public Trust Positions (SF-85P)
WWW	Personnel Security Action Request (FDIC 1600/13)
XXX	Employee/Contractor Identification Card Request (1620/01)
YYY	Declaration of Federal Employment, Submission Requirements for Contractor Personnel (OF-306)
ZZZ	Additional Background Security Questions for Contractor Personnel (FDIC 1600/25)
AAAA	Incremental Funding Chart – Update Mod 12